Technology and Communication Policy
User Agreement

Purpose

The purpose of this Technology and Communication Policy User Agreement is to provide employees, elected officials, third-party contractors, consultants, and temporary employees with the policies for acceptable usage of 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. Inappropriate use, as detailed in this document, is prohibited.

Enforcement

Employees are required to comply with the Information Technology Department (I.T.) 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 termination.

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. It is the employee's responsibility to periodically review the latest version of these policies. The employee is NOT required to submit a new acknowledgement form upon completion of a periodic review unless an updated acknowledgement is required by the employee's department.

Policy Review Guidelines

All users, as defined in Section 1 of the Technology and Communication Policy, must read, and comply with the items listed in all sections.

Employee Acknowledgement

I affirm that I have received, read, and understand the City of Pueblo's Technology and Communication Policy. I understand that violation of this policy or any misuse of computer resources is grounds for discipline or termination of employment.

____
Printed Name

____
Signature Date

INTENTIONALLY LEFT BLANK

DEPARTMENT OF INFORMATION TECHNOLOGY

Technology and Communication Policy

Version 10.0

REVISION HISTORY

REVISION NUMBER	DATE	REASON FOR REVISION	REVISED BY
1.0	11/30/2005	INITIAL DOCUMENT	I.T. DEPARTMENT
2.0	08/07/2006	UPDATED AND EDITTED FOR WEB PUBLICATION AND EMPLOYEE MANUAL DEVELOPMENT	I.T. SECURITY TEAM
3.0	10/07/2008	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
6.0	07/26/2011	REVIEW AND UPDATE TO INCLUDE SOCIAL MEDIA AND INSTANT MESSAGING POLICIES	LORI PINZ
6.1	10/12/2011	REVIEW AND UPDATE REMOTE ACCESS, GIS, AND ELECTRONIC MEDIA DISPOSAL POLICIES	GREG ROBISON MICHAEL CLARK LORI PINZ DEBI ROMINES
6.2	11/09/2011	BLACKBERRY AND EMAIL RETENTION CHANGE AND LEGAL REVIEW	CARLA SIKES LORI PINZ
7.0	09/28/2012	ANNUAL REVIEW	LORI PINZ
8.0	08/28/2013	ANNUAL REVIEW	LORI PINZ JIM KINS BETH BUKOVSKY GREG ROBISON BOB CUOMO STEVE PODSZUS DEBI ROMINES RACHEL SEIFERT MIKE CLARK
8.5	10/17/2014	ANNUAL REVIEW	LORI PINZ DAVID PETERSON WOODIE SMITH SAM AZAD
8.6	03/11/2015	CHANGE IN RETENTION POLICIES	LORI PINZ
9.0	10/17/2016	REQUIRED UPDATES DUE TO OFFICE 365 MIGRATION AND NETWORK TOPOLOGY CHANGES	LORI PINZ TREVOR GLOSS LISA MACCHIETTO MICHAEL CLARK BRIAN POPP TODD MROTEK
9.1	6/7/2018	SOCIAL MEDIA POLICY UPDATE	DAN KOGOVSEK LORI PINZ
9.2	9/28/2018	USER CREDENTIALS AND AUTHORIZED USAGE UPDATES	TREVOR GLOSS LORI PINZ
9.3	3/27/2020	ANNUAL UPDATES	LORI PINZ TREVOR GLOSS
9.4	5/10/2021	ANNUAL UPDATES	LORI PINZ TREVOR GLOSS
10.0	6/24/24	REQUIRED UPDATE. APPROVED 9/12/24.	IT TEAM ELIZABETH SEXTON-DRAKE MARISA PACHECO

TABLE OF CONTENTS

INTENTIONALLY LEFT BLANK

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 ("City") technology resources. Inappropriate use of computing resources puts the City's network, systems, and services at risk and exposes the City to legal liabilities. This policy defines standards for connecting to the City's network, telecommunications, and computing resources, as well as the security standards for computers that can connect to City's network, telecommunications, and computing resources. The Information Technology Department ("I.T." or "I.T. Department") is responsible for all technology related matters. This document does not represent all potential risks, exposures, nor does it define all the potential ways an employee could inappropriately use network resources. If an employee has concerns or questions related to the use of city's network systems and services, they should contact the Information Technology Department for assistance. Failure to do so does not absolve the employee of potential disciplinary action.

II. Scope

The policies covered in this document apply to all employees (both classified and unclassified as defined in Charter and Pueblo Municipal Code), elected officials, third-party contractors, consultants, and temporary employees employed by or utilizing technology resources of the City of Pueblo. This policy applies to all computing and telecommunication equipment that is owned or leased by the City of Pueblo. The terms of all General Regulations of the City are also incorporated herein.

III. Ownership Policy

- ➢ All components, hardware, software, or cloud-services attached to, licensed to, procured for, or installed on any City computer system or on the City's network, including but not limited to iPhones, tablets, computers, servers, laptops, and other mobile devices, are the property of the City. This does not apply to authorized personal mobile devices. Please see Mobile Device Policy below.
- ➢ The City provides computer resources, for use by its employees, for the sole purpose of conducting official City business.
- ➢ The City, as owner of said computer systems, reserves the right of periodic examination, as it deems appropriate, including but not limited to, electronic messages, call detail records, voice mail messages, data, images, or software residing on or transmitted from the City's computing resources, including electronic logs and usage records. This includes any cloud-based or 3rd party system utilized in the city to conduct city business.
- ➢ Any City employee work product produced during City employment, whether it is stored on a City-owned device or in a city licensed cloud-based system, becomes, and remains the property of the City.
- ➢ All servers and devices, i.e., iPhones, tablets etc., 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 unless a variance is approved by the IT Director and/or the Mayor.

IV. 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 can and does monitor or examine messages, data, system logs, or software that is on or is transmitted to and from its computing resources.
- ➢ Employees, as well as those parties listed above, 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, cellular phone, stored data, and phone system usage. Each employee is advised that such information is not private or confidential.
- ➢ Messages, data, or software deleted from computing resources by a user remains subject to retrieval.
- ➢ The contents of all computers, mobile devices, phone usage, call detail records and electronic mail may be subject to disclosure under the Colorado Open Records Act (CORA). 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, cellular phone, servers, etc.) are subject to public disclosure.
- ➢ The City reserves the right to block access from within its networks to any Internet site deemed inappropriate, does not meet compliance standards, or which may have a detrimental effect upon network performance.

V. 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.
- Non-Business Related: Excessive use or the unauthorized utilization of the Internet or any computing and telecommunication resource for personal use not related to job duties and work assignment.
- Employment: No employee shall knowingly delete, move, hide, or alter any data, documents, or work product to cause delay or detriment to City business or functions when terminating employment, promoting, or transferring to other City departments.
- Offensive Material: It is a violation of policy to intentionally view, create, store, print, or distribute any offensive 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, the user's job duties, or is not a copyright violation of the application or service(s). Streaming music, audio, and video services may be used by individual employees solely on their work computer as long as it is allowed by the employee's department, has no impact on employee job or network performance, and is not in direct violation of the streaming services end-licensing agreement(s). If the employee is not sure whether use of a service will violate policy, it is the employee's responsibility to contact the I.T. Department for assistance.
- Copyrighted material: It is a violation of policy to intentionally retrieve, stream, 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, non-profit organization participation and activities, 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, nor may they engage in usage which violates any rules and policies listed in this document or other official IT documents or announcements (e.g., ad hoc announcements regarding active security threats).

VI. Usage and Monitoring Policy

Employees will be granted access to the City of Pueblo's restricted information systems in accordance with their job duties. The City's restricted information systems include but are not limited to: (1) desktop, laptop, or mobile computer, (2) the computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties. All communications and data will be accessed, held, and used in accordance with applicable privacy and security policies enforced by the City. By accessing and using the City's system, employees must understand and consent to the following: (i) employees may access this information system for authorized use only; (ii) employees will only access this information system using their own credentials; (iii) employees have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system; (iv) at any time and for lawful purposes, the City may monitor, record, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and (v) any communications or data transiting or stored on this information system may be disclosed or used for any lawful purpose.

VII. Variances

The Mayor, Chief of Staff, and/or the IT 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 termination. It is the employee's responsibility to obtain guidance and approval for any use or activity that may not be listed in this document. Failure to do so may still result in disciplinary action.

IX. Acknowledgment of these Policies

Employees and elected officials are required to review and acknowledge receipt of these policies as a condition of their initial or continued employment. The City reserves the right to periodically update and require acknowledgement of receipt and understanding of this policy by covered parties as necessary.

SECTION 2 - NETWORK SERVICES AND COMPUTING POLICIES

Users on the City's network must comply with all end-user policies and use standard hardware and software supported by the I.T. Department. Requests to deviate from these obligations requires IT Director approval. The I.T. Department supports any recommended product for the duration of its life cycle. The I.T. Department is responsible for recommending, purchasing, managing, deploying, and disposing of network and computer equipment regardless of whether the department is funded as an Enterprise or by the General Fund. From procurement to obsolescence, all computer equipment is managed by the Purchasing and Information Technology Departments' policies. If the computer equipment is deemed to no longer be supportable by the I.T. Department, then it is considered obsolete and must be relinquished for data eradication. After I.T. has removed the hard drive and reusable parts, the equipment is considered surplus and must be sold or recycled by the Purchasing Department as per Charter, Article 7, Part 4, Section 7-28. f.

For assistance purchasing hardware, software, cloud-based services, network, wireless, or peripheral items, please contact the I.T. Department.

I. User Account Policy

- ➢ Any employee using technological resources will be assigned unique identification credentials (username password, FIDO key for multi-factor authentication) that allow access to various City systems and programs to perform their assigned duties. These credentials and authentication keys should always be safeguarded.
- ➢ No employee should ever allow another employee or anyone else to use their assigned credentials to access City resources or to access, view, copy, or save information they may not be entitled to under their own credentials.
- ➢ Confidential information is never to be printed, scanned, or saved onto any personal storage device, personal cloud account, or personal email account. Confidential City data should only be stored on the City's network, encrypted storage devices, or on City owned devices.
- ➢ All employees have the responsibility to take reasonable steps to protect City information, some of which is highly sensitive and confidential. Failure to take reasonable steps to secure confidential data is a violation of this policy.
- ➢ Unauthorized access to any City system or program, and/or use or dissemination of data obtained through unauthorized access, is strictly prohibited. Access gained to City systems, programs, and information using credentials assigned to another City employee without the express permission of management is also strictly prohibited. Any violations of these provision may result in disciplinary action up to and including termination.
- ➢ Generic Accounts can only be used with two factor identifications, token or biometric, and are only authorized on a very limited basis and in accord with specific criteria.
- ➢ Account information must never be shared with other City users or 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 attach 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 a City system. This username will be used for the duration of an employee's employment.
- ➢ Employees are required to use two-factor authentication methods when accessing resources via a public network.

II. User Windows Privileges

In compliance with industry standards, the City's I.T. Department adheres to the principle of least possible privilege to minimize exposure to security risks. An escalation of an end-user's privilege will only be granted if it is related to the employee's ability to perform their job functions. An end-user's privileges may be modified, changed, or revoked at any time or upon completion of an assigned task or duty. Requests for any change in privilege level (greater or lesser) must be from the employee's Department Head and approved by the I.T. Department's Security Administrator or IT Director.

III. Remote/Home Access

i. Roles and Responsibilities

It is the responsibility of the I.T. Department's network security personnel to establish, approve, or seek approval for all instances of remote access to the City of Pueblo's technology resources. Ad-hoc and non-standard VPN (virtual private network) connections are not allowed without a variance request. This request must be approved by the City's IT Director.

- ➢ In all cases, I.T. security personnel 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 by the IT Director and/or the IT Security Committee.
- ➢ Remote or VPN access for City employees must be formally approved by the employee's Department Head and the IT Director. "Remote access is subject to this Technology and Communication Policy and departmental procedures."
- ➢ Remote access for non-exempt employees may be requested by the employee's supervisor and approved by the IT Director. Based upon the request, the Mayor's approval may be required. This includes external access to the Microsoft O365 portal after-hours, while on sick leave, administrative leave, FMLA, vacation, or outside the employee's normal working schedule.

ii. Remote Access

City VPNs must be encrypted. Encryption shall be a minimum of 128-bit. Access to the City's network, whether said access is for City employees or vendors performing services for the City, will use the City's standard VPN infrastructure whenever possible.

It is a violation of City policy for employees or vendors to establish access to the City's network that has not been approved through the approval process of the City's Information Technology Department. In this context, remote access does not apply to ad-hoc sessions between City approved vendors or sales consultants and our employees using Citrix-like technology such as WebEx sessions.

Employees granted VPN access must adhere to the following criteria regarding their mobile device or home computers:

- Operating System patches must be installed in a timely manner (within a few days of release date) prior to connecting.
- Connecting systems must run current antivirus with real time protection enabled.
- Multi-factor authentication is required for all VPN access.
- Connecting systems must always run a local firewall.
- No data obtained over the VPN connection can be shared with unauthorized people.
- VPN and account credentials must always be protected. If written down, credentials must be stored in a secure location (e.g., locked container). If stored electronically, credentials must be password (complex) protected.
- Credentials are for one individual only and must not be shared with any other individual.
- Access of City systems using another person's credentials is a serious offence and may be subject to all available remedies to address such conduct.

If it is believed the VPN or LAN (local area network) credentials have been compromised, the individual must contact the City of Pueblo's Security Administrator immediately. An account compromised after-hours can be handled by calling Police Dispatch and asking for I.T. call-out to be paged.

iii. Office 365 Access

- ➢ The City utilizes Microsoft Office 365 (O365) cloud-services to provide e-mail and other Microsoft Office software applications. O365 provides on-premises access as well as on-line access using the O365 on-line portal with multi-factor authentication. The I.T. Department may control access to the on-line services based upon employee classification and work hours. In addition, each City Department has its own individual set of policies that are applicable to that specific department. Employees are expected to adhere to City policies, their respective departmental policies, as well as the I.T. Technology Communication Policy when utilizing these Cloud Services.

IV. Software Policy

- I.T. Personnel support 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, support, or otherwise fix software that was not approved by the I.T. Department.
- To ensure that I.T. can support all software installed on City computers, I.T. must approve the procurement, installation, and use of all software. This includes all on-premises and cloud-based software and solutions.
- All software on City computers or in the cloud must comply with the publishers' licensing requirements. I.T. staff will not install software or activate cloud-based applications or services unless and until ownership and proper licensing is established. IT manages the procurement of software solutions including associated licensing.
- 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.
- All software must be purchased following City of Pueblo Purchasing Guidelines. Implementation or enhancement of any City software is done by the I.T. Department.
- Microsoft application software is made available through O365 cloud-based services and is acquired through I.T. using Enterprise and volume-licensing agreements. This ensures low pricing and the appropriate version of software to address the end-user requirements.
- Microsoft Operating Systems are purchased as part of a new PC purchase and are controlled by the Enterprise Agreement with Microsoft.
- Software that is not the City's property or licensed to the City will not be installed on City computers.
- No personal software will be installed on City computers.

V. Geographic Information Systems (GIS) Standards

Information Technology supports industry standard GIS services through the Environmental Systems Research Institute (ESRI) software application suite ArcGIS Pro 3.x. The City's primary base spatially referenced information infrastructure is authored and maintained with ESRI Arc Server11.x in the form of dedicated spatial data engine (SDE) Microsoft SQL databases. Primary base data is to be authored and maintained by designated and authorized officials only. Such software and information services are available to department(s) for official use only. Should a user require functionality not available with ESRI software, but with a third-party application, department(s) and employee(s) shall be required to consult with I.T. and the GIS Division prior to procurement. Spatially referenced information products produced using City provided software and hardware shall be deemed property of the City of Pueblo and may be subject to modification by the GIS Division without notice.

Notwithstanding, all employee(s), partner(s), and/or authorized vendor(s) utilizing GIS software, hardware, and consuming spatial information resources supported by the City shall strive to provide representative and accurate spatial information. A development and metadata report shall be developed by the department(s) and their employee(s) for all spatially referenced information viewed as a primary or vital spatial information record by a department. All information request(s) submitted by a member of the public, vendor, or other governmental agency for spatially referenced information shall be reviewed and processed pursuant to standards established by the I.T. Department, GIS Division prior to release and/or distribution. For more information on end-user information standards, contact the GIS Division or I.T. Department for assistance.

VI. Computer and Peripherals Standards

Desktop Computer

- Dell OptiPlex product lines

- Dell Precision product lines

i. Notebook Computers

- Microsoft Surface Pro 8 or 9
- Dell Latitude and Precision product lines

ii. Rugged Laptops

- GETAC product lines
- Dell product lines

iii. Mobile Devices

Mobile devices will be determined based on user requirements and needs. Currently, the I.T. Department supports iPhones, iPads (in some instances), GETAC tablets, Microsoft Surface, and Windows based laptops with Broadband services provided through Verizon Wireless. The Purchasing Department is responsible for ordering and tracking of all Apple devices and cellular data plans. I.T. is only responsible for set-up and support of an Apple device. Employees shall abide by all General Regulations regarding Mobile Devices,

iv. Printers

For specific product information and guidelines for networked, shared, or stand-alone printers, contact the I.T. Department. The printer standards currently used are below; however, the 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 network laser printers for personal or individual use

VII. 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 all city computers will be configured to automatically receive virus definition updates.
- 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 use one of these services. 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.
- Use OneDrive for sharing files with outside agencies.
- Always perform a virus scan on portable media (e.g., USB mass storage devices) from any unknown source before using it.
- It is the employee's responsibility to inform the I.T. Department immediately in the event of a malware encounter.
- Responsible I.T. staff must keep virus patterns up to date either: (1) through central management or (2) if centralized management is not feasible, I.T. staff will configure the computer to download virus pattern updates directly from the anti-virus vendor.
- The I.T. Department staff will monitor the virus protection status of all centrally managed computers. Users of systems that receive updates directly from the anti-virus vendor (not centrally managed systems) are responsible for alerting IT if their systems anti-virus is not regularly updated.

- 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.
- Users are responsible for notifying I.T. if the virus protection on their system is not functioning properly (e.g., not updating).
- When virus/malware infestations are discovered, I.T. staff will examine infected systems and attempt to remediate the infection. Infected systems may be removed from the network until they are verified as malware-free by I.T. personnel.
- All employees should be aware that the city's network traffic is monitored 24 x 7 for suspicious activity by 3rd party monitoring services. In the event of a compromise or a suspicion of comprise, applications, servers and/or employee (s) computers and accounts may be shut down or removed from the network without any notice. The I.T. Department will reach out to the employee once resolution is determined.
- The City also, monitors all workstations for malicious activity which is monitored both internally and also by a third-party service.

VIII. Network Backup 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 other electronic files, should be backed up. When using One-Drive, conventional backup processes do not apply due to the multiple redundant hardware levels employed by Microsoft to support the O365 environment. The ideal approach is to store data on a City file server that utilizes a routine backup regimen or in OneDrive that relies on hardware redundancy and file versioning to maintain the integrity of files stored in OneDrive. 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.

The I.T. Department manages a back-up schedule for most information stored electronically in computerized form **except for any files kept on an employee's local computer hard drive**. Back up of local hard drive files is the responsibility of the end-user. Should the employee's hard drive completely fail, I.T. is not responsible for recovering the data. It is the responsibility of the employee to take the necessary precautions if they choose to store data on their assigned computer.

I.T. back-up processes and methodology are designed to ensure that information is not lost in the event of a severe hardware or software failure, virus attack, or other potential disaster or technological problem. Likewise, all operating software and application software necessary to access, recreate, or generate the information is also backed up. The frequency of backup depends on the significance of the information, and its frequency of change. Exceptions to backup processes exist with video recordings. For example, some surveillance video, video stored on DVRs, or cloud-hosted video do not fall under this policy. The backup devices are located between two geographical locations. Geographical distribution provides some protection against electrical failures, natural disasters, and other localized events and supports disaster recovery efforts by spatially separating the data.

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 as this provides our most-tested method of backing up your data.
- Users are responsible for backing up any data not stored on an authorized server, OneDrive, or other authorized cloud-based system.
- Personal files should not be stored on I.T. Department's file servers or in One-Drive.
- I.T. Department staff is not responsible for backing up, supporting, or restoring personal files.

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

- DVD/CD writers (not recommended for long-term backups).
- USB jump or thumb drives (encryption recommended).
- External hard drive for unusually large amounts of data (encryption recommended).

Backups containing Criminal Justice Information (CJI), or other confidential data must adhere to appropriate storage regulations. When in doubt, 256-AES encryption must be used. Backups should be performed on key data only. There is no need to back up entire desktop systems, just the data needs to be backed up. Please contact the I.T. Department for back-up assistance.

IX. Electronic Mail Policy

- **Employees are not entitled to any expectation of privacy on City resources.**
- I.T. staff shall NOT access or attempt to access another individual's e-mail box without the written permission from the individual's Department Head, Mayor, and/or the IT Director for operational continuity purposes.
- I.T. staff shall NOT access or attempt to access another individual's email box without the written permission from the Mayor or his/her designee, City Attorney or his/her designee and the HR Director when a personnel matter is being investigated.
- Recipients of quarantined E-mail messages are notified that an e-mail has been held pending release. Recipient must contact I.T. for release of quarantined e-mail.
- Treat electronic mail with the same privacy and confidentiality as physical City of Pueblo mail.
- E-mail is to be considered a form of professional correspondence 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 mail be sent to a mass distribution list.
- Do not send unsolicited mass-emails (SPAM). If you need to mass-mail, please obtain your supervisor's and the IT Director's approval.
- Do not use the City's e-mail system for political or commercial purposes.
- Do not knowingly transmit computer viruses or other malware using the City's e-mail system.
- Use of City e-mail distribution lists are for business communications only. Individual departments may restrict use or require authorization to utilize these distribution lists based upon business need and at the discretion of the Department Head.
- Notify Department Head or I.T. IT Director 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 may fall under the Colorado Open Records Act. Additionally, 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.
- An employee's City email address should never be utilized or distributed as a contact method for conducting an employee's private business with political and non-profit organizations to which they belong, unless it is directly related to City business. Obtain proper access to and documentation of e-mail by contacting the I.T. Department. Use proper e-mail etiquette. Use proper and professional language, which another individual would not find offensive, obscene, harassing, or profane. 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.
- Exercise caution regarding the content of e-mail, as messages may be forwarded to persons other than the intended recipient.
- Authorization from the IT Director is required before attaching or using an Internet electronic mail system outside City of Pueblo, e.g., Gmail, Hotmail, for City business. If an outside email is used, a method for ensuring retention and discovery under Colorado Open Records Act is required.
- Deleted e-mail correspondence, of routine value, is retained for two-years past creation date. Other e-mail correspondence, depending on its value, will be retained for a specified retention period, which may be permanent, based upon its content.
- Access to employee e-mail is controlled via City and departmental policies. All users must adhere to all applicable policies.

X. File Storage Policy

- I.T. provides space on the City's servers to store data files or on OneDrive in O365. Items that are stored on an employee's hard drive and NOT on a server may not be restorable or recoverable when the computer malfunctions. Files stored in OneDrive are not "restorable" in the conventional sense but must be restored from the user's OneDrive Recycle bin or version history in the case of file overwrite.
- Shared files (files that are commonly accessed by multiple users) should only be stored on a server, via OneDrive, or SharePoint Online, for which proper backup and recovery procedures have been established.

- Personal files should not be stored on I.T. Department’s file servers, in O365’s OneDrive, or via SharePoint services. The I.T. Department is NOT responsible for recovering lost personal files.
- Files stored in a user’s My Documents folder (or any My Documents subfolder) or via One-Drive are backed up regularly.
- Do not store any file that constitutes a copyright violation on City systems.

XI. Password Policy

- All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be a complex password with at least 14 characters. **Passphrases are preferred** (see Use of Passwords and Passphrases for Remote Users below).
- The I.T. Department enforces the use of 14-digit complex passwords as well as multi-factor authentication.
- All Police Department personnel passwords must meet Criminal Justice Information Systems (CJIS) standards in terms of complexity and the change interval.
- Standard, or non-public safety, users are required to change their passwords every hundred and eighty (180) days.
- 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 non-encrypted e-mail messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below:

i. General Password Construction Guidelines

- The password CANNOT contain the user’s account name
- The password must be a minimum of 14 characters incorporating:
  - Both upper- and lower-case characters (e.g., a-z, A-Z)
  - Digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:”;’<>?,./)
  - No elements based on personal information (names of family, etc.)

ii. Password Protection Standards

- Do not use the same password for City of Pueblo accounts and 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 support staff.
- All passwords are to be treated as sensitive, confidential City of Pueblo information.
- Don’t reveal a password in any external e-mail message.
- Don’t reveal a password on questionnaires or security forms.
- Don’t reveal a password when clicking on a link embedded in an email.
- If someone demands a password, refer them to this document or have them call the I.T. Security Administrator or IT Director
- Do not use the “Remember Password” feature of applications for any non-city related system application or service.
- If an account or password is suspected of compromise, report the incident to the I.T. Department and change all passwords immediately.

XII. Data Retention Policy

- Data must be retained per the employee’s departmental standards, with the caveat that the departmental standards must, at least, match the requirements of the Colorado State Statute for data retention.
- Data stored on I.T. supported devices will not be aged or deleted by the I.T. Department, will be backed up on a regular basis, and will be recoverable as per the guidelines below. Data may be archived in a non-destructive manner as necessary to balance data retention with cost of storage.

- When an employee terminates or leaves City employment, the employee's data and e-mail will be retained for at least 2 years, or for the retention period required, based upon the content. After the retention period has expired, all data will be destroyed.
- If an employee has been the subject of a litigation hold, as communicated by the City Attorney's office, the employee's data will not be destroyed until the litigation hold is resolved.

XIII. Electronic Media Disposal Policy

Members of the City's I.T. Department are responsible for ensuring that City media, which falls under their purview, is reused in an appropriate manner or given to the Property & Evidence Sergeant for destruction.

- The I.T. Department works with the Property & Evidence Sergeant on disposal of discarded hard drives. Discarded hard drives are incinerated/ melted.
- Non-I.T. employees of the City of Pueblo are responsible for either destroying media containing sensitive information obtained from City systems or turning media containing sensitive information obtained from City systems over to the City of Pueblo's I.T. Department for proper disposal of sensitive information.
- Through contractual obligations, City of Pueblo vendors are responsible for either destroying media containing sensitive information obtained from City systems or turning media containing sensitive information obtained from City systems over to the City of Pueblo's I.T. Department for proper disposal of sensitive information.

XIV. Media Protection Policy

Data is transmitted and stored on computer systems and electronic media by virtually every person conducting business for the City of Pueblo. Some of that data contains sensitive information, including personnel records, criminal justice information, financial data, and protected health information. If the information on those systems is not properly removed before the equipment is disposed of or transferred within the City that information could be accessed and viewed by unauthorized individuals. As such, all users of computer systems within the City of Pueblo, including elected officials, contractors, and vendors with access to City systems, are responsible for taking the appropriate steps, as outlined below, to ensure that all computers and electronic media are properly sanitized before disposal.

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.

i. Hard Drives

Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data utilizing ordinary means. All hard drives should be sanitized. However, if the drive is remaining within the City, the hard drive may simply be formatted or have an image applied prior to transfer. Special recovery tools must be used by an individual to access the data erased by these methods. Any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the City of Pueblo's Technology Communication Policy User Agreement. It is the I.T. Department's responsibility to determine the best method of managing hard drive repair, return, recovery, and destruction.

a) Sending a hard drive out for repair, return or for data recovery

- Hard drives that do not include CJI may be sent for repair. The vendor repairing or recovering data on the hard drive must sign an appropriate agreement with the City of Pueblo, ensuring that the vendor will take proper care of the data. When possible, the vendor should return the defective media for proper disposal as described in this standard.
- Hard drives containing Criminal Justice Information (CJI) should not be sent for repair in the ordinary way. The hard drive must be sent to a CJIS (Criminal Justice Information System) approved sites for data recovery.

b) Disposal of damaged or discarded hard drives

- The device must be damaged so that it is not usable by a computer. The preferred method is incineration coordinated with the Property & Evidence Sergeant

ii. Electronic media other than hard drives

Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data utilizing ordinary means. Electronic media should be overwritten if the media type allows or destroyed if overwriting is not possible (e.g., DVD).

XV. Security Policy

- Employees shall follow all the security policies and procedures established by the City; for their departments and the applications used.
- The I.T. Department reserves the right to block access from within its networks to any Internet site or technology resource deemed inappropriate or which may have a detrimental effect upon network performance. Deviation from this policy requires IT 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, iPhones, iPads, tablets, etc.) 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.

XVI. Lost or Stolen Equipment Policy

- I.T. will take appropriate steps to protect the integrity of the City’s data and security, including but not limited to, changing passwords or access to, locking access to, or to the extent possible, wiping information from any lost or stolen mobile device, including but not limited to iPhones, iPads, and laptops.
- If the device is in the employee’s possession, the employee is responsible for management and security of information residing on that device. The I.T. Department will not wipe any device in the possession of the employee unless there is a technical issue or problem preventing the device from working properly or if the device is not available or returned upon termination of employment.

XVII. Instant Messaging Policy

Instant Messaging (IM) capability is provided through Microsoft Teams, and it is currently being used as a form of real-time communication with individuals inside the organization. IM technology is meant for the purpose of enhancing employee productivity while conducting City business. However, IM carries some security risks, therefore, some functionality has been turned off by the I.T. Department.

The use of IM is a privilege, and its abuse or misuse will not be tolerated. The I.T. Department manages and may monitor all IM usage to ensure that this policy is adhered to. It is the responsibility of the user to exercise sound judgment and common sense while using IM to fulfill his or her job duties.

- **Personal Use:** Limited personal use of corporate IM services to communicate internally with colleagues regarding non-work-related matters is permitted solely at the discretion of the employee's Department Head.
- **Compliance:** IM use will comply with all City of Pueblo policies, contracts, and all applicable laws.
- **Privacy:** IM conversations and messages created on the City IM service and transmitted through City systems will be considered the property of the City of Pueblo. The City reserves the right to monitor, inspect, copy, review, store, and audit IM usage and messages generated by or for the City as it sees fit. The City may be obligated to disclose IM messages and conversations when ordered to do so by auditors, courts, CORA, or law enforcement; with or without the employee’s consent. Given these factors, employees **DO NOT** have a reasonable expectation of privacy when using City IM services.

XVIII. Video Conferencing and Collaboration Policy

The City has video conferencing and collaboration solutions available that are delivered through various methods. Desktop to Desktop or mobile capabilities exist from anywhere in the City where the end-user has a web-camera and microphone, or a mobile device available. Video conferencing units are available for larger groups in various departments throughout the City.

Microsoft Teams or Zoom are the solutions available for use. Video conferencing and collaboration tools should only be used to conduct City business and use of these tools must adhere to all acceptable use policies stated in this document.

To determine which solution is appropriate for your use, please contact the I.T. Department for assistance.

XIX. Mobile Device Policy

This policy intends to prevent data being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could be accessed by unsanctioned sources. Due to Colorado Open Records Act rules, personally owned devices are not allowed to connect to the City's network, and/or be capable of backing up, storing, or otherwise accessing City data of any type unless that access is done through the employee's O365 portal. Non-sanctioned use of personal devices to back up, store, and otherwise access any City-related data is strictly forbidden. Apple iPhone devices and Windows mobile devices are the only approved devices that will be granted wireless connectivity to the City's network.

i. Stipend Guidelines

No stipend will be provided to any employee who is using a personal device to connect to the City's network.

ii. Access and Security Control

Employees using city owned devices and related software to access the City's network and data will, without exception, use secure data management procedures. The City uses Blackberry and Intune as its mobile device management applications. The Blackberry or the Intune containers should be the only area considered secure. In addition:

- Connectivity of all City-owned devices will be centrally managed by the City's I.T. Department.
- Confidential City data should never be stored outside of the Blackberry or Intune container. At a minimum, a 6-digit PIN on the Blackberry container should be used. Password protection, combined with 6-digit PIN access, is preferred.
- Prior to initial use or requested use of the City's network or related infrastructure, **all devices must be approved by I.T.** Devices that are not pre-approved may not be connected to City's infrastructure. I.T. reserves the right to refuse connections, both physical and non-physical, of personal devices that put the City's systems, data, users, and clients at risk.
- Multi-factor authentication and strong encryption measures, or alternative compensating controls, are used to isolate and protect enterprise data accessed from or stored on mobile the devices.
- Android devices will not be allowed to connect to the City's network, due to security issues within the Android operating system.
- Any device being used to store City data must adhere to the authentication requirements of the I.T. Department. In addition, all hardware configurations utilizing enterprise data must be pre-approved by the I.T. Department prior to connecting to the City's network.
- I.T. will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. **Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt** and will be dealt with in accordance with the overarching policy.
- I.T. reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the City's network.
- In the event of a lost or stolen City-owned device, it is incumbent on the user to report the incident to I.T. immediately. City-owned devices **will be remotely wiped** of all City data and locked to prevent access by

anyone other than I.T. If the City-owned device is recovered, it can be submitted to I.T. for re-provisioning. **Appropriate steps will be taken to ensure that City data on or accessible from the device is secured - including remote wiping of the device where appropriate. The remote wipe will destroy all data on the device**, whether it is related to City business or personal matters.

iii. Help & Support

1. The I.T. Department will assist a user in determining if the issue is software or hardware related. Under certain circumstances, the employee maybe forwarded to the Purchasing Department or wireless provider for assistance.
2. Employees, contractors, and temporary staff are prohibited from making any modifications to the hardware or software that changes the nature of the device in a significant way (e.g., replacing or overriding the operating system or "jail-breaking").

iv. Organizational Protocol

1. I.T. can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the City network, and the resulting reports may be used for investigation of possible breaches and/or misuse. **The end user agrees to and accepts that his or her access and/or connection to the City's network may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity.** The end user agrees t**o immediately report** to his/her Department Head and the I.T. Department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of City resources, databases, networks, etc.
2. Users may be allowed to expense costs for mobile applications required for or used in their daily job duties. All applications and associated costs must be approved by the employee's Department Head prior to download or reimbursement.

SECTION 3 – I.T. SUPPORT STANDARDS

I. I.T. Computer Support Standards

Supporting computer software and hardware is a responsibility is generally and appropriately an I.T. function. 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 require a degree of self-support. Placement in any of the below categories shall be at the discretion of the IT 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 **pueblocity** domain. More than of 98% of the City's PCs fit into this category.

ii. Limited Computer Support – Non-Domain

This level of privilege is appropriate for users who must install software and are thus willing to support the PC themselves. Computers in the category will not be connected to the City's production domain. These PC's will be placed with the employee. 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 IT Director. In addition, I.T. will have the authority to, and will periodically audit PCs, to ensure that they do not present security exposures.

Technical Support may be delayed for users in this category. Users with this level of permissions have a more frequent incident rate and the severity of such incidents is generally greater than those without the permissions. Based upon the problem, the mean time to repair may take longer due to the greater complexity of the problem. Additional limitations apply to these systems. For example:

- ➢ No storage space on the City's servers will be provided.
- ➢ The computer CANNOT be connected to or placed on the City's network. The NIC (Network Interface Card) will be disabled to prevent it from being plugged into the City's network. The machine can have "Guest" access to the City's wireless network where available. Guest access only provides access to the City's Internet and this access can only be used to conduct City business.
- ➢ If a machine needs to be rebuilt, I.T. will rebuild the PC with a basic image. In other words, I.T. will assist with the installation of the operating system, Office applications, and virus software only.
- ➢ Fully supported and partially supported computers on the City's network will receive higher priority status than a computer in this category.

II. 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, Submit a request – City of Pueblo (zendesk.com), 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 I.T. aware of any special considerations regarding the timeliness of the response that you require.

SECTION 4 – 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. The I.T. Department must approve all telephones, telephone systems, and telephone lines. City telephones are intended for City business only and include emergency calls and calls that are in the best interest of the City. Call Detail records for all telephone calls on the City's phone system are retained for two years or until system capacity is exceeded.

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) long-distance call only in the United States; or (3) or 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. I.T. can track and audit all calls made from the city's phone system. There is no expectation of privacy related to call detail records.

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 phone services are handled through the Purchasing Department. The I.T. Department does not provide technical support for these services except for iPhone support.

IV. Order Processing and Service Requests

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

NOTE: The requesting department may be responsible for paying any charges related to their requests. I.T. will alert the department of charges prior to authorizing work. Should a department contract services outside the I.T. organization, and the I.T. 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 available to an employee in their regular course of doing business for the city. All calls made from an employee's number are tracked and can be audited at any time. There is no expectation of privacy.

VI. Phone Features

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

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

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

VII. 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 5 - NETWORK AND SERVER STANDARDS AND POLICY

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

I. Routers, Switches - Extreme Networks

- Extreme Networks is the City's preferred manufacturer for most networking equipment. As the network expands, continued implementation of the Extreme 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.

II. Network transport media

- Sites on the City's network will be connected using the City's fiber optic cable infrastructure.
- Wireless users connect using Verizon 4G/5G technology or via the City's Wireless Wide Area Network.
- 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.

III. 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.
- 256-bit AES encryption is required for remote connections. This connection is established using the City's VPN.
- 256-bit AES encryption is required for wireless connections. This is required for all Public Safety and non-public safety individuals with dedicated wireless cards.
- 256-bit AES encryption is required for Non-Public Safety wireless or Ethernet connection accessing the network with loaner computers, i.e., notebooks given to individuals traveling.

IV. Data Platforms

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

- Physical file servers provided centrally by I.T. Department.
- Virtual servers hosted through the City's virtual server environment using Microsoft Azure, VMWare and/or Hyper-V.
- Databases residing on Microsoft SQL servers.
- GIS data residing in the ESRI/MS SQL database.

V. Wireless Communications Policy

- Access is prohibited to City of Pueblo networks via unsecured wireless communication mechanisms. Guest access is available. Contact the I.T. Department for assistance with obtaining access.
- Only secured wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the I.T. Department are approved for connectivity to City of Pueblo's networks. These systems must be installed by I.T. personnel.
- Users are **strictly prohibited** from installing wireless access points that connect devices to the City's network. If found, these devices will be immediately removed.
- Systems must maintain point-to-point hardware encryption of at least 256-bits.
- Systems must maintain a hardware address that can be registered and tracked, i.e., a MAC address.

- Systems must support strong user authentication, which checks against an external database such as TACACS+, RADIUS, or something similar.

VI. Server Security Policy

i. 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 by the City of Pueblo's I.T. Department to deploy the server(s). Approved server configuration guides are established and maintained by each operational group, based on business needs, and approved by I.T.'s security administration.

Information regarding the City of Pueblo's servers is maintained within the I.T. Department.

ii. Monitoring

- On key servers, events and file access information is collected and retained to track changes and access to city data and to monitor for inappropriate activity.
- 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 and network-based attacks.
  - Evidence of unauthorized access to privileged accounts.
  - Anomalous occurrences that are not related to specific applications on the host.

iii. Compliance

- The appropriate I.T. staff will manage audits. Internal audits 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 disruption.

VII. Software Copyrights and Licensing Policy

- Ensure compliance with software license agreements by verifying that software is loaded on exactly 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 agreement.
- 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 6 – INTRANET/INTERNET SITE POLICIES

I. Intranet/Internet Site Policies

- 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 Intranet shall have the responsibility for ensuring that its material meets the standards set by the I.T. Department.
- Each department represented on the site shall have the responsibility for ensuring that its material is current.
- The I.T. Department follows the principle of least privilege for content creators and contributors to the internet and intranet sites.
- The Intranet and Internet is administrated by the I.T. Department or designated departmental staff.
- I.T. will provide standard page layout guidelines and navigations methods for use throughout the site.
- If the department 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.
- Information regarding members of City Council and other boards or commissions shall be limited to that which is necessary for Website 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 to facilitate the most efficient browsing.

i. Accessibility

The City's Website is designed and constructed to be accessible to people with disabilities and must follow Web Content Accessibility Guidelines (WCAG) (2.1 AA is the current standard). The City's Website will endeavor to meet the accessibility requirements applicable to federal departmental agencies under Section 508 of the Rehabilitation Act and the State of Colorado's House Bill 21-1110 and 24-1454.

ii. 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.

iii. Copyright and Publishing Regulation Standards

- Material on the Website may not be used in any manner prohibited by law or disallowed by licenses, contract, copyrights, or City policy/regulations/directives. Webpages 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 the content on the site.

iv. 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.
- Departments are responsible for communicating with the I.T. Department to remove any content, pages, or documents that are no longer appropriate.
- Provisions of the Fair Campaign Practices Act (FCPA) must not be violated. Material that could influence the outcome of an election must comply with the FCPA.
- Information regarding members of City Council and other boards or commissions shall be limited to that which is necessary for Website visitors to contact these individuals.

- No commercial or personal advertising of services and products is allowed on the site.
- Informational Webpages, for commercial or non-profit organizations, are permissible if such organizations have a contractual relationship with a City Enterprise (Airport, Golf Courses, Wastewater Utility, Storm Water Utility) and a fee is not collected for this service.
- Acronyms should be used sparingly and never as a first reference.
- Downloadable images should be in GIF, PNG, JPEG, or PDF format.
- Content Creator must adhere to the web accessibility policies and standards when creating and distributing any materials.
- The I.T. Department will conduct training sessions for all departments before granting any website editing permissions.
- Departments must follow the brand guidebook to maintain the color palette, logos, and structure of the page in order to ensure consistency and maintain a cohesive brand identity. This includes downloading the official log, color palette, and other brand assets. It is essential that each department ensure their materials and website aligns with the overall look and feel of the brand.
- 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 access to additional graphic images.

II. Web Architecture Standards

The City's Internet and Intranet is currently externally hosted. All components within the hosted site must comply with architecture utilized by the City's content management system.

i. Links to Other Sites

- The City's Website 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.

III. Social Networking

The City participates in social media formats, to address the changing way residents communicate, and so that the broadest possible audience is able to obtain information relating to the missions, programs, and goals of the City. All social network sites utilized by the City must be approved by the IT Director.

i. Goal

The City's goal is to open a limited public forum using social media sites to promote the economic welfare, industry, tourism, and recreation of Pueblo.

ii. Policy

- All official City of Pueblo presences on social media sites or services are considered an extension of the City's information and communications networks.
- Content placed on social media sites is monitored and archived and is subject to the Colorado Open Records Act.
- All City use of social media must be approved by the IT Director, or assigned designee, and follow this policy.
- The I.T. Department follows the principle of least privilege when managing social media contributors.
- The City may maintain as many social media sites as deemed appropriate by the IT Director for each approved social media outlet. Each social media site created shall be maintained, monitored, and regularly updated by the IT Director or any person designated by the IT Director Information Technology.
- Potential uses for social media include, but are not limited to:

  - Sharing published news releases.
  - Publicizing services and programs sponsored by the City of Pueblo.
  - Publicizing new services, holiday closings, or other information normally only found on the City's primary website.
  - Issuing emergency alerts, road closures, or weather alerts affecting large numbers of citizens.
  - Televise City Council meetings and Mayor public meetings.
- The IT Director, or any person designated by the IT Director Information Technology, will review, and approve requests to use social media sites. A request for a social media site may be denied for any reason within sound discretion of the IT Director Information Technology, including but not limited to a lack of sufficient personnel and capacity to create, maintain, and monitor the site, and/or an opinion by the City Attorney, and as approved by the Mayor that the terms of a site's license agreement are burdensome to the City.
- Use of social media must comply with applicable federal, state, and city ordinances, regulations, and policies, as well as proper business etiquette. This includes adherence to established laws and policies regarding copyright, records retention, the release of public information, the First Amendment, privacy laws, and information security policies established by the City of Pueblo.
- Wherever possible, links to more information should direct users back to the City's official website for more information, forms, documents, or online services necessary to conduct business with the City of Pueblo.
- Employees representing the City via the City's social media outlets must always conduct themselves consistently with the rules and policies of the City of Pueblo. Failure of an employee to act consistently with the rules and policies of the City of Pueblo may result in discipline, including termination, of the employee.
- The Information Technology Department, or any person designated by the IT Director, will distribute all social media content, and ensure each of the approved uses and sites adheres to the social media policy for appropriate use, message, and branding consistent with the goals of the City of Pueblo.
- Violation of the standards set forth in this Social Media Policy may result in the removal of pages from social media outlets. The IT Director Information Technology will retain the authority to remove information.
- The City of Pueblo reserves the right to remove any messages or postings that are obscene or in violation of the copyright, trademark right, or other intellectual property right of any third party.
- Social media administrators or content editors must obtain approval from the IT Director IT before removing or hiding public comments.

iii. Procedures

- All departments desiring to distribute information on the City's official social media pages shall submit a request to the Media Division of the Information Technology Department. The IT Director Information Technology, or any person designated by the IT Director Information Technology, will review the request to ensure that it meets the guidelines of this Social Media Policy, and that sufficient personnel and capacity are available to create, maintain, and monitor the social media page.
- If approved, the IT Director Information Technology, or any person designated by the IT Director Information Technology, will create, maintain, and monitor the social media site(s) approved, and will act as the official spokesperson to ensure a unified City message.
- The IT Director, or any person designated by the IT Director, will maintain a list of all approved social media sites, and will provide a link to all social media pages on the official www.pueblo.us website.
- Only City e-mail addresses or e-mails authorized in advance by the IT Director will be posted on the site or used to create the website accounts. Use of generic email addresses, for example, webmaster@pueblo.us, are appropriate to create social networking accounts.
- To the extent that design parameters of the host site allow, City of Pueblo pages will conform to the following:
  - Be identified as a City of Pueblo official site.
  - Contain appropriate staff contact information.
  - Contain the City logo or associated business logo of the City and have a link to the appropriate page of the City's website.
  - Specify that all content, comments, and replies posted will be subject to Colorado Open Records Act.

- Comply with Section 508 of the U.S. Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990 (ADA).
- Comply with the State of Colorado's House Bill 21-1110 and 24-1454.

- Departments can request social media accessibility training from the I.T. Department. Upon request, the I.T. Department will provide training materials, resources and conduct the training sessions.
- The I.T. Department monitors posts, including third party posts, across all the department social media pages on all platforms such as Facebook, Instagram, Twitter, LinkedIn, and YouTube.
- If any posts violate accessibility policies, The IT personnel will contact the relevant department and provide instructions to modify or remove the content.
- City-generated content shall:
    - Respect copyright and fair use laws.
    - Contain the following legal disclaimer:

      "The City of Pueblo encourages your comments, concerns, and questions directly relating to any of the topics on this social media site, but will remove comments that:

        - use vulgar language
        - contain threats of physical or bodily harm
        - contain personal attacks of any kind
        - contain offensive comments that target or disparage any ethnic, racial, gender or religious group
        - contain obscene or sexually explicit comments
        - incite illegal activity
        - promote commercial products or services
        - contain personal information
        - infringe on copyrights or trademarks
        - are spam, commercial promotions, or links to other sites
        - violate the law or promote the violation of law

      The City of Pueblo is not responsible for the content of, nor does it endorse, any site which has a link from this page. Please note that the comments expressed on this site do not reflect the opinions and position of the City of Pueblo. All content, comments, and replies posted are subject to Colorado Open Records Act. If you have any questions or would like to report a comment in violation, please contact us."

- The IT Director Information Technology, or any person designated by the IT Director Information Technology, will monitor each approved site, and delete any submissions, posts, or entries that violate the above disclaimer.

APPENDIX A: DEFINITIONS

City: Means the City of Pueblo

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

Destruction of Media - Destruction is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the medium, such as a computer, personal handheld device, audio, or video player.

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.

Encryption - Encryption is the process of transforming information using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

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.

Mayor: Means the Mayor or his or her authorized designee.

Media - In this document, media refers to any computer device used to store information in a non-volatile state.

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, sexual orientation, age, disability, or religious belief.

Overwriting Media for Sanitization - Overwriting is an approved method for sanitizing storage media. Overwriting of data means replacing previously stored data on a drive or disk with meaningless information. This effectively renders the data unrecoverable by standard recovery methods.

Private or Sensitive Information - Any information protected by privacy laws (e.g., CJI PII, or HIPAA) or which the disclosure thereof could result in financial loss for the City of Pueblo or which the disclosure thereof would appropriately result in a loss of confidence in the City of Pueblo by its citizens.

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

VPN - A virtual private network (VPN) is a network connection that leverages encryption technologies to secure data so that the parties can use primarily public telecommunication infrastructure, such as the Internet, and still prevent disclosure of private information to unauthorized parties.

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

Volatile - A system is said to be volatile if the information it holds is essentially lost when power is removed from the system.