CITY OF PHARR
TECHNOLOGY ACCEPTABLE USE POLICY

I. POLICY AND PURPOSE STATEMENT

1.01 City of Pharr provides some, if not all, employees with electronic access, consisting of an e- mail system, a network connection, and internet/Intranet access. These policies govern all use of the City of Pharr Network, Internet/Intranet access, and e-mail systems at all locations and offices. This policy includes, but is not limited to, electronic mail, chat rooms, the Internet, news groups, electronic bulletin boards, City of Pharr Intranet and all other City electronic messaging systems.

1.02 This policy encompasses the operation, maintenance, management of the city's radio communication infrastructure and the compliance associated with the use of and interoperability for public safety readiness.

1.03 The Information Technology Department shall charter and conduct quarterly meetings of an "Information Technology Advisory Committee" as outlined within its charter.

II. AUTHORITY

2.01 The responsibility and authority to govern the use of communications, computers and network resources is assigned by the City Commission to the City of Pharr Information Technology Department and specifically the Information Technology Director.

2.02 It is understood that failing to comply with this policy could result in disciplinary action up to and including termination.

2.03 The Information Technology Director will consult with the users department head on any disciplinary action to be taken for violations. The department director will be responsible for executing any such disciplinary action deemed appropriate.

III. DEFINITIONS

3.01 City of Pharr – local governing body known as the City Commission.

3.02 Computer Network Resources – includes computers, computer equipment, computer assistance services, software, computer accounts provided by City of Pharr, information resources, electronic communication facilities (including electronic mail, telephone mail, Internet access, network access), or systems with similar functions.

3.03 Confidential information - information maintained by City of Pharr that is exempt from disclosure under the provisions of the Texas Open Records Act or other state or federal law, attorney work product, attorney client privileged, and law enforcement communications.

3.04 Information resources – data or information, software, and hardware that render data or information available to users.

3.05 Misuse - any activity of a user or other person who engages in misuse of computing resources.

3.06 Network – a group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.

3.07 Peripherals – special purpose devices attached to a computer or computer network, such as printers, scanners, plotters, and similar equipment.

3.08 Sensitive information – administrative information maintained by City of Pharr that requires special precautions to assure its accuracy and integrity by utilizing internal departmental error checking, verification procedures and/or access control to protect it from unauthorized modification or deletion.

3.09 Server – a computer that contains information shared by other computer on a network.

3.10 Software – programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.) usually referred to as computer programs.

3.11 Network System Administrator – administrator to include the Information Technology Director and authorized staff employed by the City of Pharr Information Technology Department whose responsibilities include system, site, or network administration. Network System Administrators perform functions including, but not limited to, installing hardware, software, managing a computer or network, and keeping a computer system in operation.

3.12 User – any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one of more networks, or who attempts to connect to or traverse a network, whether via hardware, software or both. Each user is responsible for his or her use of the computer resources and for learning proper data management strategies.

3.13 Portable Data Device – any device that is considered one that communicates via WiFi, cellular data network, Bluetooth or any other manner of communication that may or may not use a public cellular carrier, for the purpose of interacting with the city's computer systems.

IV. E-MAIL

City of Pharr's e-mail system is designed to improve service to our employees, enhance internal communications, and reduce paperwork. Employees using City of Pharr e-mail system must adhere to the following policies and procedures:

4.01 City of Pharr e-mail system, network, and Internet/Intranet access are intended for business-use only. Employees may access e-mail and the Internet for personal use only during non-working hours, and strictly in compliance with the terms of this policy.

4.02 All information created, sent, or received via City of Pharr e-mail system, network, Internet, or Intranet, including all e-mail messages and electronic files, is the property of City of Pharr. Employees shall have no expectation of privacy regarding this information. City of Pharr reserves the rights to access, read, review, monitor, and copy all messages and files on its computer systems at any time and without notice. When deemed necessary, City of Pharr reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent. Extreme caution shall be use by the employee to ensure that the correct e-mail address is used for the intended recipient(s).

4.03 Employees shall attach their name to any message or file sent via e-mail.

4.04 Alternate Internet Service Provider connections to City of Pharr internal network shall not be permitted unless expressly authorized by City of Pharr and properly protected by a firewall or other appropriate security device(s) and/or software.

4.05 Confidential information should not be sent via e-mail unless clearly identified in the email as confidential by including in the e-mail the word "CONFIDENTIAL" prominently displayed, or unless encrypted by City of Pharr approved encryption software and according to established City of Pharr procedure in use at the time of transmittal. This includes the transmission of vendor financial information, Social Security numbers, employee health records, attorney client communications or other confidential material.

4.06 No employee or other may access an email account used by an employee, volunteer or other managed by the City Information Technology Department without the written expressed consent of the Information Technology Director and the City Manager.

4.07 Employees shall exercise sound judgment when distributing messages. Client-related messages should be carefully guarded and protected. Employees must also abide by copyright laws, ethics rules, and other applicable laws.

4.08 E-mail messages shall contain professional and appropriate language at all times. Employees are prohibited from sending abusive, harassing, intimidating, threatening, and discriminatory or otherwise offensive messages via email

4.09 All messages archived in City of Pharr computer systems shall be deemed property, as is all information on City of Pharr systems. Employees shall have the responsibility for verifying and understanding City of Pharr email policies as prescribed by their applicable department. Employees shall save or print messages to prevent them from being automatically deleted.

4.10 Sensitive or confidential information relating to law enforcement communications shall not be accessed without authorization for release by the District Attorney. Open Information requests for law enforcement information shall be immediately, on receipt, forwarded to the Chief of Police for its review in accordance with Chapter 552 Prosecutorial Exception, Section 552.108.

4.11 E-mails or other information relating to attorney work product and attorney client "confidential" or "privileged" information shall be protected and shall not be accessed except in strict compliance with Texas State Bar Rules, including but not limited to Rules 1.05 and 1.12.

V. NETWORK AND INTERNET/INTRANET

5.01 PERSONAL RESPONSIBILITY: By accepting an account password, related information, and accessing City of Pharr Network or Internet system, an employee shall agree to adhere to City of Pharr policies regarding their use and agree to report any misuse or policy violation(s) to your supervisor and the City of Pharr Information Technology Director.

5.02 PERMITTED USE AND TERM: Use of Network Resources and the Internet is a privilege, not a right. Use of Network and Internet access extends throughout an employee's term of employment, providing the employee does not violate City of Pharr policies regarding Network, Internet or Intranet use. Department Heads shall be responsible for the identification of both appropriate and inappropriate use.

5.03 AVAILABILITY AND ACCESS: City of Pharr reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violation, security or other concerns.

5.04 PRIVACY: Network Resources and Internet access is provided as a tool for our organization's business. City of Pharr reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of City of Pharr. An employee should have no expectation of privacy regarding them.

5.05 DOWNLOADED FILES Employees shall not download software from the Internet without the prior authorization of the Information Technology Department. Any files authorized for download from the Internet must be scanned with virus detection software before being opened.

5.06 CONFIDENTIAL INFORMATION Certain employees may have access to confidential information about City of Pharr, other employees and clients. With the approval of management, employees shall use e-mail to communicate confidential information internally as requested. Such e-mail must be marked "Confidential." For purposes of this policy, confidential information includes, but is not limited to:

5.06.01 Procedures for computer access and passwords of City of Pharr users, program manuals, user manuals, or other documentation, run books, screen, file, or database layouts, systems flowcharts, and all documentation normally related to the design or implementation of any computer programs developed by City of Pharr relating to computer programs or systems installed for the users;

5.06.02 Lists of present clients, customers, and vendors and the names of individuals at each client or customer location with whom City of Pharr deals, the type of equipment or computer software they purchase or use, and the information relating to those clients, customers, and vendors which has been given to City of Pharr by them or developed by City of Pharr, relating to computer programs an or systems installed;

5.06.03 Lists of or information about personnel seeking employment with or who are currently employed by City of Pharr;

5.06.04 Prospect lists for actual or potential clients, customers or vendors of City of Pharr and contact persons at such actual or potential clients, customers, or vendors;

5.06.05 Any other information relating to City of Pharr engineering, marketing, merchandising, and purchasing or selling of land.

5.06.06 Any information relating to attorney work product, attorney client privilege and law enforcement communications.

5.07 PROHIBITED ACTIVITIES: Employees shall be prohibited from using City of Pharr e-mail system, network, or Internet/Intranet access for the following activities:

5.07.01 Downloading software without the prior written approval of City of Pharr Information Technology Director or the direct supervisor's approval.

5.07.02 Printing or distributing copyrighted materials. This includes but is not limited to, software, articles and graphics protected by copyright laws.

5.07.03 Using software that is not licensed by the manufacturer or approved by the City of Pharr Information Technology Director.

5.07.04 Sending, printing, or otherwise disseminating City of Pharr propriety data or any other information deemed confidential by City of Pharr, to unauthorized persons.

5.07.05 Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment.

5.07.06 Making offensive or harassing statements based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

5.07.07 Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements. An employee should notify their supervisor and/or Human Resource Manager immediately upon receiving such a message. This type of message should not be forwarded.

5.07.08 Sending or forwarding a message that discloses personal information without City of Pharr authorization. This shall also include accessing, transmitting, receiving, or seeking confidential information about clients or fellow employees with authorization.

5.07.09 Sending ethnic, sexual-preference or gender-related slurs and/or jokes via e-mail. "Jokes", which often contain objectionable material, are easily misconstrued when communicated electronically.

5.07.10 Sending or soliciting sexually oriented messages or images.

5.07.11 Attempting to access or visit sites featuring pornography, terrorism, espionage, theft, or drugs; unless specifically assigned such task as part of an investigation by the Chief of Police. The Information Technology Director may assign personnel to "test" firewall rules but this action is done with written consent.

5.07.12 Gambling or engaging in any other criminal activity in violation of local, state, or federal law.

5.07.13 Participating in activities, including the preparation or dissemination of content, which could damage City of Pharr professional image, reputation and/or financial stability.

5.07.14 Permitting or granting use of an e-mail or system account to another employee or persons outside the City of Pharr. Permitting another person to use an account or password to access the Network or the Internet, including, but is not limited to, someone whose access has been denied or terminated or formally not authorized by the Information Technology Director.

5.07.15 Using another employee's password or impersonating another person while communicating or accessing the Network or Internet.

5.07.16 Intentionally introducing a virus, harmful component, corrupted data or the malicious tampering with any of City of Pharr computer systems.

5.08 REMOTE ACCESS: An employee, contractor, volunteer or other deemed authorized by the Information Technology Director and/or City Manager may remotely access the City network for official purposes only. Written request for access must be submitted via the applicable department head to the Information Technology Director for approval. Access may be granted via VPN or other secure protocol access only.

If such access is for any criminal justice data system, the Information Technology Director must seek approval by the Chief of Police prior to granting any access.

Access will only be granted to specific areas required to accomplish the official business. All remote access is in accordance with the guidelines of this policy.

5.09 PASSWORDS: An employee, contractor, volunteer or other granted use of any network resource; to include an email account must meet the following requirements regarding passwords and its use.

Passwords must be unique. It may not contain any portion of the login name or other personal identifiers. It must contain at least one special character and one numerical value. A password must be at least six characters long.

No user may possess a login/password account that does not expire. All accounts shall expire at a minimum of 90 days. The Information Technology Director may assign specific system accounts to not expire as required for engineering of network resources.

At no time should any employee, contractor, volunteer or other allow any person to know his/her password, or to login on behalf of another to any computer, tablet, phone or other device to a network resource with his/her login.

VI. COMPUTER SOFTWARE USAGE, MAINTENANCE AND EQUIPMENT

6.01 Employees shall use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except during the daily backup routine) is a violation of copyright law.

6.02 To ensure compliance with software license agreements and City of Pharr Software Usage Policy, employee shall adhere to the following:

6.02.01 City of Pharr software shall not be removed from the premises or copied for personal use. No software shall be brought into City of Pharr and installed on City of Pharr computers without a written permission of the Information Technology Director. When such permission is obtained, the software will be installed by the Information Technology Department's staff in accordance with the licensing agreement. City of Pharr Computers and supporting hardware are purchased through the City of Pharr Information Technology Department and is done so with certain criteria and standards.

6.02.02 City of Pharr prohibits the unauthorized duplication of software. Employees illegally reproducing software shall be subject to disciplinary action up to and including termination. In addition, employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.

6.02.03 Requests for new software beneficial to the mission of City of Pharr shall be made through the users department head and then approved by the Information Technology Director.

6.03 Third party/personal software shall not be installed on desktop, thin client, laptop or network computers without permission of the Information Technology Director (i.e. screen saver programs, gator, or music / video streaming software including but not limited to shareware or freeware.) Software loaded on individual computers is subject to review at any time, and unauthorized software will be removed.

6.04 If an employee is required to work or use software at home, City of Pharr shall purchase an addition copy or license if deemed necessary by the Information Technology Director or Department Head. Any employee that is issued such software shall use the software accordingly and understand that the software is the property of City of Pharr and will only be used in good order and discipline and not for non work related items.

6.04.01 Any software that has been released by the Information Technology Director for home use shall require a custody release form approved by the Department Head prior to removal from the City of Pharr premises.

6.04.02 No unauthorized personnel shall be allowed to access or use City of Pharr computers either in the City of Pharr office space or in the homes of employees.

6.05 Any employee, who knowingly installs, makes, acquires, or uses unauthorized copies of software not licensed to City of Pharr shall be subject to disciplinary action, up to and including termination.

6.06 Anti-virus software shall be installed, configured and set to automatically update on all City of Pharr computers by the City of Pharr Information Technology Department Staff, and shall not be shutdown for any reason.

6.07 Music sharing software of any kind is not permitted on City of Pharr Computers; this includes but is not limited to WINMX, KaZaa, or any of its current or legacy partners such as Napster. Furthermore, no file sharing software should be installed or enabled without the expressed written consent of the Information Technology Director.

6.08 Maintenance to City of Pharr computer / communications equipment shall be done by the Information Technology Department staff or approved outside entity. If operating system or upgrade is necessary contact the Information Technology Department staff prior to any instance, this includes but is not limited to Internet Browsers, Operating System upgrades or updates, media players, drivers or any other software not previously mentioned.

6.09 Computer Network Hubs, switches, routers, or print servers shall not be added to the network. All hardware will be approved by the Information Technology Director prior to the procurement or installation of any network hardware.

6.10 Any personally owned computer, smart phone, iPOD, iPAD or other such device shall not be connected to City of Pharr Network unless specifically connected to "PUBLIC" networks. The use of such devices on the "PUBLIC" network are not protected in any manner. No employee should utilize the "PUBLIC" network in excess during work hours and is not expressed any expectation to privacy while operating on such network.

6.11 Computers (i.e. Desktop, Thin-Client, Servers, or Laptops) as a whole are considered one device, the replacement, addition, or removal of any internal / external component to any such entity is strongly prohibited. If more memory, hard disk, or repair to any item is needed, contact the Information Technology Department.

6.12 Telecommunications equipment and services shall be procured and configured through via the Information Technology Department. Contact the Information Technology Department if addition, repair, maintenance, or relocation of telecommunication services are required, this includes but is not limited to phone, cable services, T1, fiber optic and similar services

6.13 The City recognizes that many City employees use social media tools such as Facebook, LinkedIN, Twitter, etc in their business and personal lives. Therefore, this provides guidelines for City employees when they communicate on social media sites while being employed:

6.13.01 The use of social media sites during work hours should be done for official city business only, using city owned computer devices. The use of social media websites is authorized during break periods as long as such access is not done via any city owned computer or smartphone.

6.13.02 The department head must approve any creation of a social media site presenting that specific department. At any time, the Information Technology Director may remove or make unavailable any social media website representing the city; if it is deemed necessary by the City Manager.

6.13.03 No employee, while on city time or not, may place any derogative statement about the city or any statement which may reflect negatively on the city or the employee in their official capacity. This is to include any posting of a personal or public nature on any site that may or may not require a login to view such statement.

VII. ENFORCEMENT - COMPLIANCE AND NONCOMPLIANCE

7.01 Management personnel shall be responsible for ensuring employee compliance with City of Pharr Policy and shall immediately report the violation to their direct supervisor, Department Head, Information Technology Director and/or the Personnel Director.

7.02 Violation of these policies shall result in disciplinary action up to and including termination. It is important to note that failure to adhere to this Policy may lead to the cancellation of a user's computer account(s), suspension, dismissal, or other disciplinary action by City of Pharr as well as referral to legal and law enforcement agencies.

VIII. MOBILE DEVICES / USE OF AND USE OF PERSONAL DEVICES

8.01 The City allows for, but does not support/warranty the use of a personally owned computer device / smart phone being used for official city business. Such use by any employee, volunteer, contractor or other is subject to the following stipulations while such device contains any data belonging to the City.

8.01.01 The user shall maintain an anti-virus software on such device.

8.01.02 The user shall maintain a lock on the device which requires a unique password and/or PIN to access the navigation screens.

8.01.03 The user shall notify the Information Technology Department if the device is lost or stolen. The user understands that if the device was used to connect to the city email system, that the device may be erased to avoid any possible leakage of sensitive data. The user understands that all data would be lost if this process is completed. The city is not liable for any damages associated with the erasing of the device or failing to erase the device.

8.01.04 The City will not be liable in any way for the value of any device used by an employee for work performed or any usage charges associated with such work being completed.

8.01.05 Any City data stored on the device must be removed upon request by any member of management or the Information Technology Department. The user is reminded that all stored data originating from or deemed part of the City is the sole property of the City and subject to all other areas of this policy.

8.02 The City may revoke the users privilege to use a personal device at any time, with or without cause.

8.03 All portable tablets / computers / cell phones / smart phones owned by the City are for official use only. Great care should be exercised to ensure that such devices remain free from unnecessary damage while being used / stored. Users are reminded that any device owned or funded by the City has no expectation of privacy and is open to applicable search / seizure according to policy and / or law.

8.04 At no time shall any user possess or remove from inventory any portable data device belonging to the city without authorization of their applicable department head and / or the Information Technology Director. All portable data devices owned or funded by the City must be checked out via approved paperwork and be inventoried accordingly.

IX. PURCHASING

9.01 The Information Technology Department; specifically, the Information Technology Director shall be responsible for approving all technology related purchases / contracts / services for the City.

9.02 Any department head has the authorization to purchase consumable printing supplies for existing printers in place within his/her department. The department head must comply with all applicable purchasing guidelines.

9.03 Any department head needing to add / modify / remove any technology equipment, services and contractual obligations must first have the Information Technology Department review such request and seek approval before incurring any costs associated with such action.

9.03.01 The department head requesting such action is responsible for completing all requirements of action and then shall forward a memorandum stating the reason for the request, any applicable funding sources necessary for the action.

9.03.02 The Information Technology Director will review, verify and process or forward for review any approved requested action in accordance with the purchasing policy, to the City Manager / City Commission.

X. TWO-RADIO COMMUNICATIONS

10.01 The Information Technology Department shall be responsible for the specification, purchasing, and maintenance of all two-way radio communication devices owned by or operated on a frequency licensed to the City.

10.02 Any user of a radio agrees to do so in a professional manner at all time and in compliance of all Federal Communication Commission rules and regulations.

10.03 Any user of a radio agrees to maintain such device in a safe manner and agrees to report any damage or problems with the device to the Information Technology Department for repair.

10.04 At no time will any user or radio be permitted to use proprietary encryption or methods of communications, which is not approved by the Information Technology Department. AES/DES-OFB encryption is permitted for use as deemed necessary.

10.05 Encryption keys / algorithms shall be maintained in an encrypted format and not released to any persons outside of the City unless such action is required for official business and authorized by the Information Technology Director in writing. Such action will be authorized only if consulted with the Chief of Police. No repair vendor will possess any encryption algorithms, devices possessing City encryption at any time.

10.06 All departments that have been issued or has purchased radios will maintain an accurate inventory of the location of the radios and who they have been issued to for use. In the event a radio is lost/stolen, the department will notify the Information Technology Department in a timely manner to have that radio disabled in the radio system to prevent its unauthorized use.

10.07 Any person engaged in communications on common channels, or interoperability channels will reframe from the use of codes. This includes 10-code, signal codes and others. Clear text is required to ensure that effective and direct communications occur to avoid miscommunications between multiple disciplines operating on the same channel.

10.08 The Information Technology Department will be responsible for developing, maintaining and testing a disaster plan associated with procedures to be executed in the event the City radio system fails. This information will be disseminated to all department heads.

10.09 The Information Technology Department will perform quarterly audits of radio traffic on the City radio system. The audit will look for unauthorized use of the system by those not authorized to use as well as monitor the usage to facilitate capacity planning and address growth issues before they become a problem.

XI. GEOGRAPHICAL INFORMATION SYSTEMS (GIS):

11.01 The Information Technology Department shall be responsible for the GIS operations for the City and shall appoint a manager within its department for overseeing data storage / management.

11.02 The GIS Manager shall meet regularly with departments to address needs and review data to ensure its accuracy. No employee outside of GIS is authorized to change data without review from GIS. This is to ensure that the data maintains accurate and accordance with local, state and national standards.

11.03 Address issuance, changes and updating of information with 911 is the responsible of the GIS Manager. No other department / division may issue or manage addresses within the city.

11.04 The GIS Manager shall maintain an online resource of maps and tools available to all departments and residents of the city. GIS shall provide training to city employees

The following is a list of some laws that pertain to computer usage, the list is not encompassing:

1. Texas Administrative Code, 202: Information Security Standards

2. Texas Penal Code, Chapter 33: Computer Crimes

3. Texas Penal Code, Chapter 37: Tampering with Government Record

4. United States Penal Code, Title 18, Chapter 47 Fraud and False Statements, Section 1030: Fraud and related activity in connection with computers.

5. Computer Fraud and Abuse Act of 1986
6. Computer Abuse Amendments Act of 1994
7. Federal Copyright Law
8. Digital Millennium Copyright Act of 1998
9. Electronic Communication Privacy Act 1986
10. Computer Software Rental Amendments Act 1990
11. Homeland Security Act H.R. 5005 November, 2002