PERSONNEL POLICY - 180.00 TECHNOLOGY - ACCEPTABLE USE POLICY

The City of Hagerstown provides access to vast information resources that enable users to do their job quickly and intelligently. The facilities to provide that access represent a considerable commitment of City resources for telecommunications, networking, software, hardware, storage, etc.

This Acceptable Use Policy is designed to help staff understand the expectations for the use of those resources and to help them use those resources wisely.

SCOPE OF POLICY

This policy applies to all employees of the City of Hagerstown whether employed in a permanent, temporary, or contract capacity, including full-time, part-time, seasonal, interns, grant participants, external partners conducting business with the City, and elected officials.

For the purpose of this policy, the term "user(s)" refers to all persons identified in the preceding paragraph and the term "City" refers to the City of Hagerstown.

SECTION I - INFORMATION TECHNOLOGY REQUESTS

A. All project based information technology requests need to be requested through the Director of Information Technology and Support Services. All operational requests (problems, HW/SW installations, etc.) are to go through the Help Desk.

SECTION II - HARDWARE AND SOFTWARE

A. All hardware and software purchases, including but not limited to; computer systems, printers, scanners, copiers, mobile devices, etc., must be purchased and technically ratified through the Information Technology Department. This ensures that IT can:

- Manage all technology resources for the City
- Produce an accurate inventory of our assets
- Provide overall reduced costs of ownership
- Guarantee standards and operability

Exceptions to this rule should be made only after consultation with the IT Director.

B. Users with Internet access may download to their computer only software with direct business use, and must arrange to have such software installed by IT, licensed and registered. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. Special requirements must be approved by the IT Director.

C. Users with Internet access may not distribute any software licenses to the City or data owned or licensed by the City without explicit authorization from the IT Director. Users must be aware that the data they create on the City's systems remains the property of the City. All electronic documents and correspondence (electronic mail, faxes, etc.) are corporate records. The City reserves the right to access and disclose as necessary all messages sent over its computer systems, without regard to content. Information should not be stored or transmitted that the user would not want to be read by a third party.

SECTION III - TECHNICAL

A. The City Human Resources Department will provide IT with information to setup a new employee on our system. The employee will be provided secure access to their computer, email, time and attendance system, and any other secured system needed to complete their job responsibilities.

B. The User ID and password will be provided to Human Resources and communicated to the employee during orientation.

C. The IT Department has the authority to reset/disable a user's password when requested by the specfic user or their supervisor. The supervisor will provide direction on how to handle the employee's account if/when they leave the employ of the City.

D. All mobile devices connected to the City network must have a password to gain access.

E. The City has installed firewalls, Internet screening programs and other security systems to assure the safety and security of the City's network. Any user who attempts to disable, defeat or circumvent any City security process may be subject to disciplinary action.

F. A user is NOT to provide their password to another employee for access to the City network. If required to provide to the IT Department to resolve a problem, it is recommended that they change their password once the issue is resolved.

G. All PC's, laptops and mobile devices should be secured with a password-protected screensaver when being left unattended.

SECTION IV - INTERNET AND EXTERNAL EMAIL USAGE

A. The Internet access for City employees is a business tool. It is expected that users will use their Internet access for business-related purposes, i.e., to communicate with clients, citizens and suppliers, to research relevant topics and obtain useful business information.

B. While the connection to the Internet offers a wealth of benefits, it can also open the door to some significant risks to the City's data and systems. Security is to be the user's first concern. Internet users can be held accountable for any breaches of security or confidentiality. Incidental use of the Internet for personal use is limited to breaks and must follow the Acceptable Use Policy.

C. Users are advised to conduct electronic mail messaging in the same manner as they would other business correspondence; being mindful of the fact that electronic mail is subject to the provisions of the Public Information Act (PIA).

D. If a user is accidentally connected to a site that contains explicit or offensive material, disconnection from that site must occur immediately and immediate supervisor notified.

E. The City as a provider of access to communication systems reserves the right to specify how the City's network resources will be used and administered to comply with this policy. While not all-inclusive the following behaviors are examples of actions which DO NOT meet the definition of "appropriate use" and are in violation of this policy unless these actions are required as part of an employee's duties:

a. Downloading, displaying or distributing any explicit, discriminating, threatening, harassing or offensive graphic or document. In addition, explicit material may not be archived, stored, distributed, edited or recorded using the City network or computing resources.
b. Deliberately propagating any virus, worm, Trojan horse, or trapdoor program code into the network.
c. Knowingly participating in chain letters, pyramid schemes or email spam (any scheme that would encourage the uncontrolled generation of email), messages of a political or religious nature, solicitations unrelated to City operations, or otherwise offensive material or language.
d. Knowingly downloading or distributing pirated software or data.
e. Downloading entertainment software or games, or playing games over the Internet
f. Installing of instant messaging or video messaging programs should be limited to those authorized in the IT Department.
g. Emails on the City of Hagerstown's system are considered official communications. To maintain uniformity, employees who are authorized to use email will refrain from using quotes, logos, or other characters and symbols <u>unrelated to City operations</u> unless directed by the City Administrator.

F. POLICY COMPLIANCE MONITORING

A. The City is committed to preserving its reputation and making its presence safe and secure on the Internet. To ensure this, IT will maintain the right to properly monitor all Internet users in order to ensure compliance with the City's Acceptable Use Policy.

B. The City will comply with lawful requests from Human Resources, Law Enforcement, and regulatory agencies for logs and archives on individual's Internet activities.

C. The City reserves the right to inspect any and all files stored in private areas of its network in order assure compliance with the policy.

D. All City business related documents, files and email messages created, received, stored in, or sent from any mobile device are considered public record.

SECTION V - INTERNAL EMAIL

A. The **EVERYONE_MAIL** group found in the City's address book is setup for business related purposes only and restricted to designated staff members.

B. To reduce the impact to storage space and bandwidth, graphics and attachments should not be used unless required as part of an "urgent" communication such as weather, security, phone, technical, or other.

SECTION VI - PASSWORDS

A. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the City's entire network. It is important that all users take the appropriate steps to ensure that the password chosen is unique and secure.

B. Poor, weak passwords have the following characteristics:
   a. The password is a common usage word such as wife's name, pet's name, etc.
   b. The password is a single word found in the dictionary.
   c. Birthdays or other personal information such as street name or phone number.
   d. Word or number patterns such as "abcdef", "123456", "abc123".
   e. Any of the above spelled backwards.

C. Strong passwords include:
   a. Contain both upper and lower case characters.
   b. Have digits and punctuations as well as letters.

c. Passwords should never be written down or stored online in an unsecured way. Use of a password keeper is permitted with encryption.

D. Do not share a password with anyone, period. Do not reveal a password in an email or helpdesk request. Only communicate a password to IT if requested, and then do it personally on the phone or in person. Do not hint about a password, reveal the password on any questionnaires or forms, share with family members, or provide to a co-worker if leaving for an extended vacation.

E. Do not use the "REMEMBER PASSWORD" feature of Internet Explorer or Google Chrome.

F. If you feel a password has been compromised, contact the IT Helpdesk immediately.

SECTION VII - REMOTE ACCESS

A. The ability to remotely access your office computer from an outside location will be provided only with the approval of that staff's supervisor and/or Department Head and the IT Director.

B. The staff requiring remote access capabilities will meet with the IT Director or Network Administrator to receive software and instructions for setting up access to the office computer. Any issues the staff person has with setup should be directed to the Network Administrator as soon as possible. The setup CD will not be shared with any other staff person, and will be returned as soon as successfully installed to the IT Department. Failure to comply with this policy may result in disciplinary action as spelled out in City policy.

C. All external computers accessing City computers should be up-to-date with latest anti-virus and malware software. Free software may be downloaded via the Internet to the home computer for installation. Contact the IT Department for information.

D. Storage of confidential City information on any non-City owned device is prohibited. Confidential information may not be stored on any portable device (jump drive, removable storage, etc.) without prior approval from the Department Head. Approved storage of confidential information on any portable device must be encrypted or password protected.

E. All individuals and machines, including City-owned and personal equipment, are a de facto extension of the City's network, and as such are subject to the City's Acceptable Use Policy

SECTION VIII - CITY TABLET USE

A. The City will provide tablet use to staff at the discretion of the City Administrator.

B. The City will issue a tablet with wireless / cellular technology installed and configured, including a tablet cover for the unit's protection.

C. Any other accessories will be purchased by the user at their own expense.

D. All tablet users, due to the portability of the unit, will be required to sign a tablet use agreement, approved by the IT Director.

E. Tablet users are responsible for the general care of the unit. If the tablet is broken or fails to work properly, the unit will need to be delivered to the IT department for troubleshooting. Do not affix any labels, stickers, etc. to the unit unless used as inventory identification for tracking purposes.

F. Standard software will be provided on the device to allow the staff person to perform the necessary requirements of their job. City Council members will have access to the NOVUS Agenda and Meeting system for access to work packets and other information related to an official meeting.

G. Any software, email message or file downloaded via the Internet on the unit will become the property of the City and may only be used in ways that are consistent with applicable licenses, trademarks or copyrights. Files from sources where there is reason to believe may be untrustworthy shall not be downloaded, nor shall files attached to email transmissions be opened and read unless the user has confidence they originate from a reputable source.

H. Staff will return all tablets to the IT Director upon separation from their City employment. The tablet will be delivered to IT, where it will be wiped clean of all information and restored to its default configuration.

I. The tablet will otherwise be covered to the covenants set forth in this Acceptable Use Policy and/or Work Rule 19.

SECTION IX - FAILURE TO COMPLY

A. Failure to comply with the provisions of this policy may result in disciplinary action per City policy.

EMPLOYEE CERTFICATION FOR USE OF TABLET COMPUTER POLICIES / RESPONSIBILITIES

Tablet computers are assigned to City of Hagerstown employees whose need for mobile computing is of an essential nature in the conduct of City business.

Authorized users are responsible for knowing how to properly operate the device, basic care and troubleshooting as trained, and understanding and adhering to al copyright requirements related to software used on the device.

Authorized users are responsible for reimbursing the City for the purchase price of a lost or stolen tablet if its loss or theft is due to their negligence.

Authorized users will ensure that the tablet is secure at all times, especially when used in a public place. The device will not be left unattended unless physically secured.

Authorized users understand that all information on the tablet may be subject to Public Information Act requests and/or Public Meeting laws.

Authorized users are responsible for returning the tablet to the City Information Technology Department when it is no longer required to carry out their City work assignments. Staff must reimburse the city for the purchase price if they do not return the tablet, or if the unit has been broken or neglected.

Employees violating these procedures are subject to disciplinary action.

EMPLOYEE CERTIFICATION

I have read and understand the requirements stated above and in the mobile device policy and agree to adhere to them.

Name of Authorized User: _____

Signature of Authorized User:

City Department Employed In: _____

Department Head Signature:

Tablet Serial Number: _____

Personnel Policy 180.00
adopted: June 2, 1997
Rev: November 1, 2006
2nd Rev: April 1, 2015
3rd Rev: Nov. 1, 2015