HAMPTON VA

No. IT– 020	Policy Name: Acceptable Use Policy
Effective Date: 7-1-2011 Last Revised Date: 7-4-2014	Citywide Policy X IT Policy _ IT Procedure _
Approved By: IT Director	

Acceptable Use Policy

1.0 Overview

The goal of the Acceptable Use Policy (AUP) is to protect the City of Hampton's IT assets and provide guidance to all employees on proper use for equipment and network services. Information Technology's intentions for publishing an AUP for Hampton is not to impose restrictions that are contrary to the City of Hampton's established culture of open-ness, trust and integrity. IT is committed to protecting employees, partners and the city from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, soft-ware, operating sys-tems, storage media, network accounts providing electronic mail, web browsing, social media and file or data transfers are the property of the city. These systems are to be used for official city business purposes in serving the interests of the city, and of our citizens in the course of normal operations. Please review Human Resources Policy Chapter 2.2 for further details.

Effective security is a team effort involving the participation and support of every city employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. Being informed is a shared responsibility for all users of the City of Hamp-ton's information systems. Being informed means, for example:

• Knowing these acceptable use policies and other related rules and policies

• Knowing how to protect your data and data that you are responsible for

• Knowing how to use shared resources without damaging them

• Knowing how to keep current with software updates

• Knowing how to report a virus warning, a hoax, or other suspicious activity

- Participating in training

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment on the City's computer network. These rules are in place to protect both the employees and the City. Inappropriate use exposes the city to risks includ-ing virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

Compliance with this policy is mandatory for all city officials, employees, agency, boards, committees and contractors of this organization. Police IT and it users are also included in this pol-icy. For the purposes of this document, this group of individuals will be referred to as —Usersll. This policy also applies to all information, computer systems and data that are used for official city business regardless of its location. This policy applies to all equipment that is owned

eased by the city. This policy also applies to all individuals who operate this equipment. In addition, users must still abide by local state and federal laws and regulations as well as established city policy while using computer systems. Examples include, but are not limited to:

- Laws governing copyright and intellectual property
- State regulations regarding document retention http://www.lva.virginia.gov/agencies/records/
- Laws concerning privacy and freedom of information
- City of Hampton, 2006 Technology Management Guide – This will be updated as new policies are developed

4.0 Policy

General Use and Ownership

1. While the IT Department desires to provide a reasonable level of privacy, users should be aware that the data they create on city systems remains the property of the City of Hampton. Because of the need to protect the city's network, employees should have no expectation of privacy regarding the use of the City's technology systems.

2. Users are responsible for exercising good judgment regarding the reasonableness of sys-tem use. Users should be guided by IT policies on such use, and if there is any uncertainty, employees should consult their director, manager, supervisor or IT Help desk.

3. All technology systems usage is subject to inspection to ensure compliance with city policies; any suspected breeches of security shall be audited by the City Manager or designee at any time with or without notice.

4. Many of the Information Systems used by the City require passwords. Users passwords should NEVER be shared with anyone, including members of IT staff, nor should any efforts be made to obtain the password of another user. If anyone requests your password, this activity should be reported to the department's Director and IT Director immediately.

5. Anyone that connects to the City Network will be assigned a unique user name and pass-word and is expected to maintain their password. The sharing of user accounts to log onto systems is not permitted.

No attempt should be made to obtain a level of rights on a system beyond what has been ex-pressly granted. Examples of this include attempting to log onto a system with another user's login name, accessing an ap-plication or system through back-door access, or the use of hacking tools.

Workstation Use

1. Users should never leave their workstations in an unprotected state. If a user anticipates being away from their PC or workstation, they should either log off of their PC or lock it by pressing CTRL+ALT+DEL and selecting "Lock Workstation". Screen Saver passwords, which will lock a workstation once a screen saver is activated, are highly recommended. Screen savers should be set to activate after 10 minutes or less of inactivity.

2. Any applications installed on a user's PC must be approved by IT and directly related to fulfilling their job responsibilities. New applications must work without requiring administrative rights on PCs or workstations.

3. Members of IT Technical Support and Engineering staffs maintain administrative level access to all network-connected PCs on the City network. Attempts to block or override this level of access are prohibited.

4. Any foreign media (CD-Roms, USB flash drives, removable hard drives, etc.) will be scanned for viruses or other malicious content before files are opened or copied from them. Users can contact the IT Helpdesk (727-6421 or ithelp@hampton.gov) for assistance.

5. Anti-virus and/or Anti-malware software will be installed on every PC attached to the city network. Users are prohibited from interfering with the operations of this software. This includes attempts to uninstall or disable the software.

6. Each user has been allocated disk space on a network file server for storage. Users can access this storage by selecting their Z: drive in Windows Explorer. Users should save their documents to their network drive to ensure that they are backed up for disaster recovery purposes. Network storage space is for work related information only. Content of a personal nature should not be stored on network drives.

Local Area Network Use

The Information Technology Department maintains a robust data/telecommunications network which enables users to conduct business as efficiently as possible. This network joins all city-owned PCs on a common communication platform, as well as enables Internet communication.

PCs and other network-based devices, such as printers, can only be attached to the network with approval from IT.

The connection of personal devices to the City network is prohibited unless approved by the IT department. This includes but is not limited to printers, faxes, monitors, PCs, laptops, storage devices, and network devices.

The IT Department is solely responsible for configuring devices to communicate on the network. Attempts to override IT configured settings are prohibited. IT may designate and approve individuals to configure devices. IT will require proper training and process compliance before the designation is approved.

Network expansion devices, such as wireless access points, switches, or hubs, are installed and managed exclusively by IT. These types of devices, when purchased through local retail stores, are designed for home use, and can introduce significant security vulnerabilities to the City network. Installation of these devices by anyone other than IT staff is prohibited.

Only select members of IT staff are allowed to actively monitor the City Network. The use of network monitoring tools by non-IT staff is prohibited.

Remote Access Use

1. IT provides a number of Remote Access and Virtual Private Network (VPN) solutions to its users. These are the only approved remote access services to connect to the City of Hampton's network. Department heads or their designee will approve all user remote access requests. These approved services include:

a. Client-Based VPN - This solution provides a seamless connection between the remote user's PC and the Hampton internal Network. This is the most secure and stable solution the City provides.

b. Web-Based SSL VPN – This solution allows a user to make a secure connection to the inside of the City's network.

c. Remote Access PC Software – This solution is a 3rd party solution for Remote Access. This solution allows for a user to install a small application on their office PC which then makes a connection to an Internet based server. This user can then make a connection from any PC to the same Internet server to establish a remote session to their desktop at work.

d. When a user requests a new Remote Access Connection, City IT will work with the customer to select the best solution based on user needs and security requirements.

e. Any user who is connecting to the City network from their home PC is responsible for the security settings of that PC. This includes ensuring that Antivirus and Anti-malware software is installed and up-to-date with the latest definitions, and that Windows Updates are current. The IT Department may refuse any user the right to use their home computer for access to the city's network.

f. Vendors that require Remote Access will be provided with a client-based VPN solution. IT will support WebEx or GoToMeeting style sessions when a member of the IT staff is available to attend and view the session while the vendor is connected. Vendors will be required to complete and return a "Letter of Agreement for Remote Access to the City of Hampton Network" to the IT Department before Remote Access will be provided.

The use of 3rd party Remote Access tools (including GoToMyPC connections not coordinated through IT) to establish either an inbound or outbound connection between and external PC and a PC on the City network is prohibited unless approved by the IT Department.

Internet (Web) Use

1. Web browsing and social networking activity should be limited to business-related sites..

2. Sites that stream video or audio are generally not permitted from the City network unless there is a business need.

3. IT maintains a web filtering appliance that monitors web-related traffic on the network. IT actively blocks the following types of contents. Department heads or their designee may request access to blocked sites for employees where it is necessary for business functions.

a. Sites known to contain malware/spyware/adware
b. Advertisements/Pop ups
c. Adult and pornography
d. Confirmed span sources
e. Known hacking sites and sources
f. Keyloggers and monitoring
g. Nudity
h. Online gambling
i. Proxy avoidance and annonymizers
j. Phishing and other known fraud sites
k. Online personal storage
l. Instant messaging
m. IT can generate activity reports for any user when requested by a Department Head.

n. If IT discovers in the course of troubleshooting a network or PC related issue that an user's web activity is adversely affecting normal business operations, this will be reported to the appropriate manager/ Department Head.

o. Sensitive information should never be entered onto a 3rd party web form unless the site is secure. Users can quickly identify a secure site by locating a small lock icon on the bottom of their web browser. If there is any doubt, the user should contact the IT Helpdesk for assistance.

p. Instant Messaging utilities contain a large number of security vulnerabilities, and are not permitted on the network, unless a user provides a defined business need for such a service.

q. The use of P2P (peer to peer) services are prohibited. Examples include BitTorrent and LimeWire.

Electronic Mail (Email) Use

1. Email should be used for business use only.

2. Email is not designed for the transfer of large files. Files larger than 10 MB should not be sent using email. If a user must transfer a larger file to a user or a group of users, they should contact the IT Helpdesk for alternate methods.

3. Chain emails and spamming are an abuse of the City's email system, and are not permitted. This includes spreading email without good purpose to an individual, group, or system.

4. "Bombing", which is the flooding of users, groups, or systems with large email messages, is not permitted.

5. The use of the "City Employees" distribution group should be limited as much as possible and should be only for business reasons. Please consult with your manager prior to using this group for any communication.

6. The "IT Department" distribution list should not be used to report issues. All IT-related issues should be reported to ithelp@hampton.gov.

7. Spam is unsolicited email sent from a 3rd party agent outside of the city. IT maintains a spam-filtering appliance, which attempts to filter out junk email from a users' inbox. However, since all Spam filtering solutions are rules based and reactive, no spam solution is full-proof. Therefore, if a user is repeatedly receiving unsolicited email, this email should be forwarded to spam@hampton.gov and then deleted.

8. Phishing is a type of malicious email that appears to be from a legitimate source, such as a financial institution, that requests that you click on a web link and enter in sensitive personal information. Attackers then use the information provided to engage in identify theft. As with spam, IT actively filters phishing emails intended for city employees. However, if you do receive this type of email, simply delete it. Users may also opt to forward the e-mail to spam@hampton.gov for further investigation and to notify other at risk departments. You should NEVER respond to any email that is requesting any of the following items:

a. Social Security number

b. Credit Card numbers

c. Passwords

d. Bank account numbers

e. Information specific to the City's network or telephone system.

f. Spoofing is a technique used for spam and phishing, where the sender makes it appear that the email originated from a different source. The email may appear to be from you and also to you, or it may be to you but is not from the apparent sender. Attackers use these spoofed emails to get you to click on virus links, and also to obtain personal information from you. If you suspect you have been spoofed, simply delete the email.

Users on the Microsoft365 e-mail service have a mail storage limitation of 25GB. Email deletions should be made in accordance with the state's records retention laws. Please see the City's records Management Manual for more specific guidance on email deletions and retention methods.

5.0 Social Networking Use—Marketing Inc Review

Social networks are online communities of people or organizations that share interests and/or activities and use a wide variety of Internet technology to make the interaction a rich and robust experience. Examples of social networking services include blogs, Facebook, MySpace, LinkedIn, Twitter, Second Life and many others. This also includes forms of online publishing, discussion groups; file sharing, user generated video and audio and virtual worlds. Employees that choose to participate in social networks as a City employee shall adhere to the following.

1. City policies, rules, regulations and standards of conduct apply to employees that engage in social networking activities while conducting City business. Use of the City's e-mail address, website and communicating in your official capacity will constitute conducting City business.
2. Departments have the option of allowing employees to participate in existing social networking sites as part of their job duties. Department heads may allow or disallow employee participation in any social networking activities in their departments for business use.
3. Protect your privacy, the privacy of citizens and the information that the City holds. Follow all privacy protection laws like HIPPA and protect sensitive and confidential City information.
4. Follow all copyright laws, public records laws, records retention laws, fair use and financial disclosure laws and any others that might apply to the City or your functional area. Contact the City's Records Manager by contacting the IT helpdesk (ITHelp@hampton.gov) if you have any questions on records.
5. Do not site vendors, suppliers, clients, citizens, co workers or other stakeholders without their approval. When you do, make a reference and where possible link back to the source.
6. Make it clear that you are speaking for yourself and not on behalf of the City. If you publish content on any website outside of the City of Hampton and it has something to do with the work you do or subjects associated with the City, use a disclaimer such as this: "The postings on this site are my own and don't necessarily represent the City's positions or opinions."

7. Do not use ethnic slurs, profanity, personal insults, or engage in any conduct that would not be acceptable in the City's workplace. Avoid comments or topics that may be considered objectionable or inflammatory.

8. If you identify yourself as a City employee ensure your profile and related content is consistent with how you wish to present yourself with colleagues, citizens and other stakeholders.

9. Correct your mistakes, and don't alter previous posts without indicating that you have done so. Frame any comments or opposing views in a positive manner and don't pick a fight or harass others on the Internet.

10. Add value to the City of Hampton through your interaction. Provide worthwhile information and perspective.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.