	POLICY & PROCEDURE	SERIES # **534**	PAGE 1 OF 7
	SUBJECT **AUTOMATED SYSTEMS USE**		EFFECTIVE DATE **11/13/2019**
			OVERSIGHT **Fiscal Management**
	DISTRIBUTION **ALL MANUALS**	AMENDS/SUPERSEDES/CANCELS P&P # 534 dated 10/03/17.	

I. PURPOSE:

This policy establishes guidance concerning the installation, operation, maintenance and security of the computer systems in support of the Hampton Police Division. Computer systems are defined as those components of hardware, software and communications interfaces that support Hampton Police Division functions. Software is a set of instructions the computer uses to do a series of tasks.

II. POLICY:

The Hampton Police Division maintains computer systems support to provide for increased effectiveness and efficiency of work effort, storage of data and access to other information systems through communications interfaces. It is the policy of the Hampton Police Division to: 1) control the configuration of computer systems; 2) distribute software only in accordance with license agreements; 3) ensure security and privacy of data stored on computer systems operated by the Division, and 4) limit the use of police computer systems to official police business and other uses as permitted by the Chief of Police.

Furthermore, system use is governed by Division policies, City policies, local, state and federal laws. Use of systems owned and operated by the Division will: 1) be ethical; 2) be constrained in the consumption of shared resources; 3) demonstrate respect for official information, ownership of data, and system security mechanisms; 4) be respectful of individuals' rights to privacy and their rights to freedom from intimidation and harassment.

See City Policy: IT-020 “Acceptable Use Policy” for additional information.

III. PROCEDURE:

A. <u>USE OF SYSTEM</u>

1. The Police Systems/Information Technology (IT) Section provides network administration and development services to the organization. All aspects of the Division wide area network to include system planning, development, network communications, software, hardware, end user training, and equipment installation are coordinated through this activity.

2. All reports or information that have been created via an automated system and that will be publicly disseminated MUST be approved by the Chief of Police or his designee to ensure that the information complies with all local, state and federal laws.

3. Personally identifiable information (PII) includes Social Security Numbers, credit card numbers and pin and driver's license numbers of citizens, employees, suspects and others. This information shall not be copied, stored or uploaded to any non-HPD IT managed system or device unless approved by the Chief of Police or his designee. The HPD Network Manager or his designee will oversee the transfer of any PII data outside of HPD IT systems and storage devices. The last four digits of credit card numbers can be displayed in any reports or correspondence. The last four digits of social security numbers can be displayed for any reports or correspondence. Additional PII guidance is as follows:

   a. Data or reports that contain the full SSN, full credit card number, or other PII will not be stored, maintained or uploaded to any locations or devices that are used as public web portals or open data portals even if those systems are secure and password protected.

   b. Data or reports that contain the full SSN, full credit card number or other PII will not be stored, sent or received via e-mail, text messaging, social media, FTP or other non- HPD IT managed methods.

   c. Data or reports that contain the full SSN, the full credit card number or other PII will not be generated, stored or maintained on individual PCs, laptops, or handheld devices. This type of data should only be stored and maintained in the official applications and network storage devices utilized by HPD and managed by Police IT. Exceptions to store this type of information on individual devices must be approved by the Chief of Police.

   d. PII should only be stored in HPD applications in the fields and areas designated for that purpose. PII should not be stored in text fields or other description fields not specifically identified as containing PII.

   e. Information that is destined for a public portal will be reviewed after creation but before publication by the Chief of Police or his designee as a second check to ensure no PII is present.

4. In making appropriate use of Division computer resources users are to:

   a. use resources only for authorized purposes.

   b. protect against the unauthorized use of USER ID (members are responsible for all activities conducted on their USER ID or system).

   c. access only files and data that are your own, that are available to the public, or to which you have been given authorized access.

d. use only legal versions of copyrighted software in compliance with vendor license requirements.

e. be considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer paper, manuals or other resources.

f. E-mail messages to be distributed City Wide must be approved by the distributing individual's Unit Commander prior to distribution being made.

5. Unacceptable Practices

a. installing software or hardware without the System Administrator's permission.

b. modifying computer systems files, such as modifying the autoexec.bat, config.sys and systems folders.

c. using screen savers or other program components with passwords which prevent others from making use of the system.

d. displaying, playing or transmitting materials that may be considered offensive by others.

e. granting or otherwise allowing access to any Division computer or automated system by any outside agency or individual(s) without the express written permission of the Chief of Police is prohibited.

f. making, storing, using or distributing illegal copies of copyrighted software using the Division's systems or network.

6. Prohibited Uses

a. using another person's USER ID, password, files, system or data without permission.

b. using computer programs to decode passwords or access control information.

c. attempting to circumvent or subvert system security measures.

d. engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services or damaging files.

e. using Division systems for partisan political purposes, such as using electronic mail to circulate advertising for political candidates.

f. making or using illegal copies of copyrighted software, store such copies on Division systems or transmit them over Division networks.

g. using mail or Messaging services to harass, intimidate or otherwise annoy another person.

h. using the Division's system for personal gain.

B. ENFORCEMENT

Violators are subject to disciplinary action as prescribed in the City Employee Manual, Rules and Regulations and Division Policies and Procedures. Offenders can also be prosecuted under laws including (but not limited to) the Civil Rights Act of 1871 (Title 42 U.S.C., Section 1983), the Privacy Protection Act of 1974, the Computer Fraud and Abuse Act of 1986, the Computer Virus Eradication Act of 1989, the Virginia Computer Crimes Act and the Electronic Communications Privacy Act.

C. SYSTEM CONTROLS

1. INVENTORY CONTROL

a. The System Administrator maintains records of computer system hardware and software.

b. Periodic inspections and inventories are performed to ensure that computer system hardware and software components are maintained and accounted for.

c. Isolated automated systems are periodically inventoried by the Unit Commander responsible. The inspection ensures that all components, media and documentation are properly secured and maintained.

d. Individual users store and control expendable materials.

e. Software magnetic media and associated documentation is controlled and stored by the System Administrator.

2. SYSTEM SECURITY

a. All users log off the Division net when they will be away from their system for an extended period or if their system is accessible to unauthorized users.

b. All users log off at the end of the work day using proper

procedures for the system.

c. IT security is a shared responsibility of the City of Hampton IT Department together with HPD IT. One ongoing security initiative by City IT is to ensure that all network access accounts have policies applied to require password changes every 90-days and require that passwords meet a city-standardized length and complexity requirement.

Employees will be notified via e-mail by the system that their password is about to expire 14 days out. It will be the employee's responsibility to go into the system and change their password. Passwords must meet system requirements. If not changed it will result in the employee being locked out of the system and they will need to contact Police Helpdesk for further assistance.

Cyber security is built on a "Defense in Depth" concept that includes many layers of protection. No single layer can provide complete protection and this makes user education and account security (setting and protecting passwords) critical layers in protecting city resources.

d. The System Administrator will conduct routine backups of systems and data to maintain disaster recoverability.

D. COMMUNICATIONS INTERFACES

1. Users must not use the computer system facilities to send obscene, vulgar, intimidating or harassing messages.

2. Offensive materials take many forms in the world of computing and networking. Originators have a responsibility to monitor their material so that it is not obscene, vulgar or harassing. Users do not store offensive materials (i.e., messages, pictures or suggestions) or download them to the Division system.

E. SOFTWARE

1. All software for use on Hampton Police Division automated systems is approved for use by the Systems Administrator. Software must work without administrative rights.

2. The unauthorized copying of copyrighted software is illegal. Users who make and use illegal copies of software are subject to civil and criminal penalties, as well as Division sanctions and disciplinary actions.

3. Division software media is maintained by the System Administrator in a secure area away from general access.

4. Software purchase requests are coordinated and routed through the

System Administrator. Submissions are justified to provide a basis to establish priorities and identify software needs. This ensures that the software, once received, is installed on the appropriate server and provides coordination of purchases from a limited budget.

5. All software development for the Division is coordinated through the System Administrator.

F. EQUIPMENT

Computers and other devices that plug into or utilize the Police Networks are the responsibility of Police Systems. These devices are not considered property of the units where they are located. Relocation of computers and devices must be requested and coordinated with Police Systems.

G. TRAINING

The Hampton Police Division assists employees with improving and developing computer skills through a variety of computer training programs. Training is achieved through individual user assistance, in-house training courses and contract training.

1. Individual User Assistance - Knowledgeable unit personnel are to make themselves available to assist less knowledgeable users in mastering routine tasks. Additional assistance is also available from personnel from other units that are educated computer users.

2. In-house Training - User training sessions sponsored by the Division and the City is held periodically in the Emergency Operations Center. Trainers are sourced from Division and City personnel. Notice of available training sessions is coordinated through Training. This training is specific to the Division and City computer applications and is geared toward system and application orientation and task proficiency.

3. Contract Training - The Division utilizes contract training through area software training firms for specific advanced application training. Notice of available training sessions is coordinated through Training. Users interested in attending training submit a Training request for the appropriate course(s).

G. DISSEMINATION OF INFORMATION

Criminal History information from any of the Divisions computerized systems shall be used only for the Law Enforcement purpose for which the request was made. Dissemination of such information outside of it's intended Law Enforcement use will result in disciplinary action, and possible criminal prosecution.

H. REPORTING SYSTEM PROBLEMS

1. In order to maintain consistency in resolving IT related problems for users Central IT in the Police Division was established as Police Systems.
2. Since the Police Systems personnel are frequently busy with repairs and installations, a system has been put into place which will allow them to better serve everyone. Police Systems has instituted a standardized procedure for all requests and concerns regarding computers and related equipment.
    a. All users experiencing a problem or requesting assistance are to email their request for service to policehelpdesk@hampton.gov
    b. Include a complete description of the problem or request. For example, if the problem involves a printer the request must include the printer and its location.
    c. The Police Systems unit will respond within two business days to the request. They will make every effort to respond as soon as possible. However, the maximum two day response window is necessary for them to prioritize requests for service from all units and Divisions.
3. When immediate assistance is required to maintain operational readiness, users should notify their supervisors who may contact the Police Systems Supervisor by phone.

-