ST. PETERSBURG POLICE DEPARTMENT	DATE OF ISSUE	EFFECTIVE DATE	NUMBER
GENERAL ORDER	November 2020	Immediately	**II-17**
	Distribution: All Employees		

Subject: **COMPUTERS, SOFTWARE AND ACCEPTABLE USE OF DEPARTMENTAL INFORMATION SYSTEMS**

Index as:

- Authorized Software
- Backup, Data Use and
- CDs
- Computer
- Computer Virus
- Data Use and Backup
- Documentation
- DVDs
- Electronic Mail (Email)
- Electronic Messaging
- Email
- FAC
- FCIC Agency Coordinator (FAC)
- Flash/Memory Cards (Sticks)
- Hard Drives
- Hardware
- Hardware, Computer
- Internet, Use of
- Laptop Computers
- License
- Magnetic Tapes (USB, SCSI)
- Media
- Mobile Computers
- Mobile Public Safety (MPS)
- MPS
- Network
- Network, Computer
- Operating System
- Passwords
- Personally Owned Devices
- Removable Media
- Security
- Shareware
- SIM
- Smart Cards
- Software
- Software Acquisition
- Software, Computer
- StPeteWiFi_MobileMe Agreement
- Subscriber Identity Module (SIM)
- Transitory Electronic Message (Email)
- Unauthorized Data or Files
- Wireless Usage
- Zip disks or drives

Accreditation Standards: 11.4.4, 41.3.7, 82.1.6

Cross Reference:
- G.O. III-8, National and State Criminal Justice Information Systems
- G.O. II-46 Securing and Protecting Physical and Electronic CJI Data
- ECD SOP IV-01 Service Channel Operations
- City Administrative Policies 070300, 070400, 070500, 070800
- Chapter 119, Florida State Statutes

Replaces: G.O. II-17 Computers, Software, and Acceptable Uses of Departmental Information Systems (December 5, 2022)

This Order establishes guidelines and procedures related to obtaining and operating hardware including mobile data terminals, software and the appropriate installation and use of these devices and programs. This Order consists of the following sections:

I. Policy
II. Definitions
III. Purchase of Hardware and Software
IV. Data Systems Ownership
V. Laptop Computers
VI. Wireless Usage Restricts/Logs
VII. Electronic Mail and Messaging
VIII. Use of the Internet
IX. Service and Repair
X. Enforcement

I. POLICY

A. It is the policy of the St. Petersburg Police Department to use all computers, computer software, networks and related devices in accordance with all applicable criminal and civil laws and City policies. Additionally, all licensing agreements delineated by the software publisher will be complied with.

B. The Information and Technology Services Division (ITS) will perform periodic audits including, but not limited to, hardware, software, Email, Internet use, etc., to ensure compliance with the policies contained within this Order.

C. The St. Petersburg Police Department does not allow multiple concurrent sessions of Department information systems.

II. DEFINITIONS

A. Authorized Software – Software that:

1. Is purchased by the City or the Department, or

2. The City or the Department has a site license, or

3. Is in the public domain.

B. Computer – An electronic device which uses a set of instructions (software) to perform various functions.

C. Documentation – Written instructions and/or licensing that:

1. Accompanies software at the time of purchase, or

2. Is prepared by the ITS, or a supplier, that gives instructions or establishes the procedures to be followed when performing a function, or using an application provided by a computer or information system.

D. Electronic Messaging – Any electronic mail service, including Email, which provides facilities for creating, transmitting, and displaying messages on computers; or the individual messages created using any electronic device through the use of such a messaging service or the Internet.

E. Freeware – Computer software that is made available to computer users free, similar to shareware but with no cost associated at all. The software often has conditions attached (*i.e.*, the software cannot be modified, may be time limited, etc.).

F. Hardware – Visible parts of a computer including desktop, mobile/laptop or handheld devices; usually includes the monitor, keyboard, installed or removable disk (hard) drive(s) and the housing which stores the internal components. Other hardware includes printers, modems, wireless data cards, switches, cables, media storage devices and network equipment, etc.

G. Laptop Computers – Laptop computers, also known as MDT, are portable computers that provide the user the opportunity to take it with them for use in different environments.

H. License – A written agreement by the software publisher and agreed upon by the software user, stating how the software may be used, the number of copies which may be made, how many users may use the software at any one time, and any other requirement the software publisher wishes to be part of the agreement. There is usually implied agreement to the license requirements when the user breaks the seal to the software package or when a user selects the “I Agree” option during the installation of any software package or download.

I. Media – Any removable or transportable data storage medium. Removable media examples include, but are not limited to:

1. CDs

2. DVDs

3. Flash/Memory Cards (Sticks)

4. Hard Drives

5. Magnetic Tapes (USB, SCSI, etc.)

6. Smart Cards

7. Subscriber Identity Module (SIM)

8. Zip disks or drives

J. Mobile Public Safety (MPS) – Mobile Dispatch Application used by field personnel with real-time maps and event details for better incident management and situational awareness.

K. Network – A connection of several computers by cables, radio, fiber optics, wireless services, microwave or other means to allow the transfer and sharing of files and/or software installed on one or more of the computers.

L. Operating System – Instructions and programs used to cause a computer to perform various functions. (See also Authorized Software.)

M. Personally Owned Devices – Cell phones, tablets or any other device that is owned and maintained by the user, and not by St. Petersburg Police Department.

N. Shareware – Computer software that is made available to computer users free, or at a very low cost, for the purpose of evaluating the software before purchase or registering with the software publisher.

O. Software – Computer instructions/programs used to cause a computer to perform various functions. (See also Authorized Software)

P. Transitory Electronic Message (Email) – Messages that, by their nature, quickly become “obsolete, superseded, or their administrative value is lost.

Q. Unauthorized Data or Files – are those that have not been created on the Department’s internal information systems during the course of business or those which have been supplied by any outside source and have not been subjected to security and/or virus screening. Such files include those that have not been approved by the Chain of Command or which do not further any official purpose.

III. PURCHASE OF HARDWARE AND SOFTWARE

A. Hardware

1. The purchase/lease of any computer hardware and/or any peripheral device must be reviewed and approved by the Assistant Director, Administrative Services Bureau (ASB).

2. ITS will ensure that all hardware is properly inventoried in coordination with the Fiscal Services Division; assigned an asset number; and accurate records maintained of all hardware and peripheral devices, whether they are stand-alone, installed within, or attached to any other computer or device.

3. No communications devices, such as modems, wireless data cards, or WiFi devices will be connected to any Department computer without the written approval of the respective Assistant Chief and the Assistant Director, ASB.

4. Hardware will not be transferred from the person or organizational unit to which it is assigned, without the approval of ITS and submission of the required fixed asset transfer documents to the Fiscal Services Division.

B. Software

1. Software Acquisition

a. Purchased Software

1) Purchase requests will be approved by the Assistant Director, ASB to ensure the software is appropriate for the purpose intended, compatible with the hardware in use, and standardized throughout the Department.

b. Software acquired other than by direct purchase, as further described below will, in all cases prior to installation and after any review by the Legal Division and/or the City's Department of Technology Services (DOTS), be examined by the ITS Division to determine that it is appropriate for the purpose intended, compatible with the hardware in use, and standardized throughout the Department.

1) Commercial software provided to the Department, other than by direct purchase (*e.g.*, grant funded or on loan, etc.), must have the licensing requirements reviewed by the Legal Division and must be submitted to the City's Department of Technology Services (DOTS) for security review and virus screening. Prior to installation, the software will be submitted to ITS for examination and approval.

2) Shareware must be reviewed and approved by ITS prior to installation on any Department system.

3) Freeware must be submitted to ICS for security review and virus screening. Prior to installation, the software will be submitted to ITS for examination and approval.

4) Public domain software must have the licensing requirements reviewed by the Legal Division and must be submitted to ICS for security review and virus screening. Prior to installation, the software will be submitted to ITS for examination and approval.

2. All software will be procured through ITS and will follow current budget and purchasing procedures regarding the purchase of software.

a. Any purchase exceeding $100.00 will be properly inventoried and assigned a City asset number.

b. Software media and documentation will be handled as defined in this Order.

3. All original software media and documentation (licenses, installation "key," etc.) will be kept by ITS.

a. If the media is required for the software to function, the original or a copy may be provided to the user as determined by the Manager, ITS.

b. City-owned software will not be:

1) Copied, except as permitted by the license agreement;

2) Installed on any personally owned computer unless authorized by the Manager, ITS;

3) Manipulated or altered in any manner on any City-owned mobile, desktop or handheld computer.

4. All software registration documents will be properly completed in a timely manner, showing the owner as the St. Petersburg Police Department, and returned to ITS.

5. All personally owned software, software considered to be in the public domain, shareware or freeware may not be installed/used on a Department computer, unless:

a. Written permission is granted by the Assistant Director, ASB; and

b. The licensing agreement allows for the installation; and

c. The data stored and used by the software is available for export in a format acceptable for use by other software used in the Department.

C. ITS will support the goals of the Department by providing recommendations and approval of computer hardware, peripheral devices and software, along with support and maintenance of the Department's computers and networks.

IV. DATA SYSTEMS OWNERSHIP

A. General Use and Ownership

1. Employees who are assigned or have access to a Department computer will use the equipment in professional manner for official business only and comply with all laws and City policies related thereto.

2. All computers and computer software will be used in accordance with the applicable licensing agreements.

3. Only authorized software will be used on any Department computer.

4. Users must be aware that the data remains the property of the Department. Most business records, including electronic records are subject to Florida's Public Records Act, Chapter 119, Florida Statues.

5. Users must not use the Department's information systems, which include computer systems, Internet, intranet or network, for personal use.

6. For assistance with the transmission of sensitive or restricted information as defined in the Florida Public Records Act, users should call 727-551-3200 or Email the Department's Help Desk at PD.HelpDesk@stpete.org.

B. Police Department personnel will only be authorized to access third party law enforcement information systems in accordance with agreements and laws governing access to those systems.

V. LAPTOP COMPUTERS

A. A laptop computer is issued to all Sworn and identified non-sworn members as needed.

1. The computer will have the data stored and encrypted on removable disk drives.

2. The computer will be operated in strict compliance with Department written directives, City of St. Petersburg Rules and Regulations, rules and procedures in the operations manuals issued by ITS and the policies of the local, state and federal networks to which the computer has access.

3. Safeguards will be taken to avoid viewing of sensitive or confidential data by unauthorized persons who may be in a position to view the screen while in a public place or in the vehicle.

4. The laptop computer and related media, portable computing devices and removable components will be secured in order to prevent theft and to protect them from damage that may be caused by sharp objects, liquids, etc.

5. In- car Laptop Users

a. The computer will be used for law enforcement purposes only and will supplement the voice communication systems.

b. The computer will be installed in the vehicle mount, powered on, and logged into the Mobile Police System (MPS) software at all times when the Officer is on duty and is assigned a vehicle.

c. When working an off-duty assignment, the computer will be installed, powered on, and logged into I/mobile at all times when the Officer is assigned a vehicle.

d. An Officer assigned a vehicle under the take-home car program will have the computer properly installed in the vehicle, powered on, and logged into MPS any time the vehicle is used for official or personal use as permitted by Department policy.

B. Information from FCIC/NCIC

1. FDLE/FBI CJIS data is sensitive and will be treated accordingly. Any unauthorized request for receipt or release of information could result in criminal proceedings.

2. Information received from FCIC/NCIC will be requested for criminal justice purposes only.

a. Criminal case history (CCH) information is strictly limited to a law enforcement purpose. It will not be shared with others not involved in the investigation, nor sought for the personal benefit of the employee. Sharing or using information for anything other than job-related criminal justice duties constitutes a violation of user privileges.

b. Voice transmission of CCH information should be limited, and details should only be given over a radio or cell phone to ensure an Officer's safety, or if it is determined there is a danger to the public.

c. Officers are not permitted to print any CCH information. A printed copy, if required, must be logged and disseminated from either an Echo Channel operator or the Records and Evidentiary Services Division FCIC/NCIC operator.

3. All transactions between the mobile computer and FCIC/NCIC are monitored and tracked at the Department, state and federal levels.

a. The FCIC Agency Coordinator (FAC) conducts a bi-annual audit to confirm information is requested and accessed properly and adheres to FDLE policies and procedures related to criminal justice information.

b. Employees accessing FCIC/NCIC for a CCH will provide the reason for each inquiry upon request.

VI. WIRELESS USAGE

A. Employees who have been assigned a Department-owned cell phone and will be using the Department's Wi-Fi, will review and acknowledge the StPeteWiFi_MobileMe Agreement located in CARS under Web Links.

B. Employees who use their personally-owned mobile device (cell phone, tablet, laptop, etc.) to connect to the Department's Wi-Fi, will review and acknowledge the StPeteWiFi_MobileMe Agreement located in CARS under Web Links.

C. ITS will monitor all connections and audit logs associated with the devices as well as the systems and applications that the devices access. ITS will review these audit logs monthly or more frequently if there is an increased risk to St. Petersburg Police Department information or systems.

D. Employees are prohibited from accessing Department systems on any public wireless network without connecting to the Department Virtual Private Network (Netmotion) for authentication.

1. The access to the information systems is only allowed for job-related functions.

2. Users are not permitted to attempt to add, remove or modify any hardware, software, network devices or other information systems in place within the Department. If the user requires additional hardware, software, or network devices to perform duties related to their current job function, the user must contact ITS to request the addition.

VII. ELECTRONIC MAIL (EMAIL) AND MESSAGING

A. The electronic message system and all messages created therein are property of the City and are intended to be used solely for City business purposes.

1. Legitimate uses of electronic mail and messaging include the following:

a. To facilitate performance of job functions and to facilitate the communication of information in a timely manner.

b. To communicate with departments throughout the City and to outside organizations, as required, in order to perform job functions.

c. Incidental and occasional personal use of e-mail is permitted by the City and will be subject to the same restrictions as other communications.

2. Prohibited uses include, but are not limited to:

a. Illegal activities, release of confidential information, threats, harassment, intimidation, slander, defamation, obscene or suggestive messages, offensive graphical images, or political endorsements.

b. Also prohibited is use of the e-messaging system to send copies of documents in violation of copyright laws, to compromise the integrity of the City and its business in any manner, or to use the electronic message system for outside or secondary employment ("moonlighting"), job searches for non-City jobs, or the advertisement of personal business.

B. Electronic Mail (Email) Messages are Public Records

1. Electronic messaging (Email) is monitored and recorded.

2. Electronic messages are, in most cases, considered a public record and subject to release.

3. Unless an Email message meets the criteria to be considered "transitory"; *i.e.*, those messages that, by their nature, quickly become "obsolete, superseded, or their administrative value is lost," it must be retained in a manner that complies with Florida State Statutes.

4. For Email messages that are required to be retained:
   a. If the Email message is internal to the City's Email system, it is the sender's responsibility to comply with the retention requirements of the Records and Information Management Program established by §257.36, F.S.S.
   b. If the Email message originates from an Internet user, it is the responsibility of the recipient to comply with the records retention requirements of §257.36, F.S.S.

5. For all Email messages which meet the criteria to be considered a public record, the Department is required to allow access to any person upon request.
   a. A person need not have a “legitimate” need for public records to be entitled to inspect them.
   b. State and federal law exempts certain categories of documents and, in some cases, certain types of information within a document from disclosure under the Public Records Law.
   c. Before any Email is released pursuant to a public records request, any exempt information must be redacted.

6. Deleting Email messages from one’s own computer does not delete it from various internal and external files.

7. Personal Email message accounts with on-line services should not be accessed from Department computers.

8. When an employee leaves the Department, ITS will:
   a. Archive files and/or folders containing correspondence, documents, data, etc., that were created and/or utilized by the employee.
   b. Maintain these archives as required by applicable public records laws.

VIII. USE OF THE INTERNET

A. The Internet is a valuable tool. Employees will maintain a diligent and professional working environment when accessing the Internet.

B. The Internet is not to be used for activities which are perceived to be illegal, harassing, offensive, or in violation of other department or City policies, or any other uses that would reflect adversely on the department or the City.

C. Internet access is provided for official business only. Employees may not use the Internet for personal gain, gambling, or to access any obscene or pornographic sites; and they may not access or use information that may be considered harassing or offensive to others, without the approval of the Chief of Police.

1. Employees requesting Internet access will review the City of St. Petersburg Administrative Policies, Utilization of Technology:
   a. https://stpsp1/sites/csp/Intranet/HumanResources/Shared%20Documents/AP070300.pdf
   b. https://stpsp1/sites/csp/Intranet/HumanResources/Shared%20Documents/AP070400.pdf
   c. https://stpsp1/sites/csp/Intranet/HumanResources/Shared%20Documents/AP070500.pdf
   d. https://stpsp1/sites/csp/Intranet/HumanResources/Shared%20Documents/AP070700.pdf
   e. https://stpsp1/sites/csp/Intranet/HumanResources/Shared%20Documents/AP070800.pdf

2. View the Internet video on CARS.

3. After viewing the Internet Video on CARS, the employee will electronically sign the *Internet Use* Agreement on CARS.

D. Requests for Undercover (UC) internet access for high security areas such as Strategic Operations Division, Intelligence, and other special operations will made to the Department’s Help Desk at PD.HelpDesk@stpete.org.

E. Personal Internet accounts with online services will not be accessed from Department computers; e.g., e-mail, blogs, webpage, etc.

F. Misuse of the Internet will result in discipline up to and including termination.

IX. SERVICE AND REPAIR

A. All installation, repairs, removal and/or relocation of computer hardware and software including, but not limited to, network peripherals, cables, printers, scanners, etc., will be performed by ITS.

B. Employees will neither remove nor authorize the removal of hardware, software or storage media from the computer to which it is assigned, without approval of their supervisor.

C. Employees requiring hardware or software repair, installation or other services should call 727-551-3200 or Email service requests to the Department's Help Desk at PD.HelpDesk@stpete.org.

1. Service requests will be assigned a trouble ticket number and handled by priority and in chronological order.

2. For follow-up inquiries, the employee should provide the trouble ticket number to ITS.

D. Employees will immediately notify ITS of any incident involving the loss of a device, loss of control of a device, or a device being compromised.

1. ITS will initiate steps to resolve the incident and mitigate the risk to the Department by disabling the computer in Active Directory to prevent any unauthorized access.

2. In addition to the steps outlined in G.O. II-12 Negligent Damage Loss or Theft of Department Property, the Department will use email to expedite the reporting of security incidents.

X. ENFORCEMENT

A. Violation of this Order may result in:

1. Suspension or termination of an individual's or organization's right of access to Department information systems.

2. Disciplinary action, up to and including termination.

3. Referral to law enforcement authorities for criminal prosecution, or

4. Other legal action, including action to recover civil damages and penalties.

B. Non-enforcement of any policy or procedure herein does not constitute consent or waiver, and the Department reserves the right to enforce such policy or procedure at its sole discretion.

_____
Anthony Holloway
Chief of Police