General Order

Houston Police Department

ISSUE DATE:	NO.
June 19, 2015	400-25

REFERENCE: Supersedes all prior conflicting Circulars and Directives, and General Order 400-25, dated October 2, 2006

SUBJECT: ACCEPTABLE USE OF COMPUTERS

POLICY

Except as provided by this General Order, all *computers* or *networked systems* owned, leased, rented, or under the control of the department shall be used for business purposes in serving the interests of the city. Except as provided by this General Order, any data (e.g., file, program, email) created (whether on- or off-site) on a department owned or controlled *computer* or *networked system* is the property of the department.

This General Order applies to all employees, including all authorized personnel affiliated with third parties (see General Order 800-06, **CJIS Compliance**).

DEFINITIONS

Computer. For purposes of this General Order, computer includes, but is not limited to, any personal computer, laptop computer, tablet computer, smartphone, or any other device that is owned or controlled by the department and is capable of accessing network or Internet resources.

Disruption. This term includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Networked System. For purposes of this General Order this term refers to any department owned or controlled Internet, Intranet, or Extranet related systems. This also includes workstations, desktops, laptops, tablets, or server systems, and the hardware and software to operate those systems.

Malicious Programs. Viruses, worms, email bombs, Trojan horse codes, or other destructive or disruptive programs.

Security Breach. This term includes, but is not limited to, accessing data the employee is not intended to receive or logging into a computer, server, or account the employee is not expressly authorized to access.

Spam. Unauthorized or unsolicited messages sent to a large number of recipients via the Internet. Also, the act of sending *spam*.

1 DIRECTIVES

All *networked systems*, computer equipment, software, operating systems, and storage media, as well as network accounts providing email, Internet browsing, or file transfer protocols that are owned, leased, rented, or controlled by the department are to be used for business purposes in serving the interests of the city and users in the course of normal operations. The City does not prohibit the limited use of a *networked system* for personal use. Brief personal usage of 3-5 minutes to check email, the weather forecast, or news sites are examples of acceptable use of department computers for personal reasons. However, employees are responsible for exercising good judgment regarding personal use.

Each office, command, division, and unit is responsible for creating guidelines concerning the use of department owned or controlled computers and *networked systems*. In the absence of such policies, employees shall be guided by department regulations regarding personal use. If there is any uncertainty, employees shall consult with their supervisor before using a *networked system*.

2 AUDIT INFORMATION

For security and network maintenance purposes, authorized individuals within the department may monitor equipment, *networked systems*, and network traffic at any time. The department reserves the right to audit any department owned or controlled *networked system* on a periodic basis to ensure compliance with this policy.

3 SECURITY AND PROPRIETARY INFORMATION

Any information accessed via a *networked system* may be classified as confidential (e.g., law enforcement private information, organizational strategies, specifications, telephone and contact lists, and research data). Employees shall prevent unauthorized access to this information. See also General Order 800-06, **CJIS Compliance**.

Employees shall keep passwords and personal identification numbers (PINs) secure and shall not share accounts (see General Order 400-22, **Keys, Passwords, and Personal Identification Numbers**). Authorized users are responsible for the security of their passwords, PINs, and accounts. System level user passwords and PINs shall be changed every 90 *calendar* days.

Any computer that connects to a *networked system*, regardless of who actually owns the computer, shall be:

a. Protected and continually scanned by approved anti-virus software.

b. Maintained to current levels of protection.

c. Configured to obtain operating system patches and updates from the Office of Technology Services or an authorized software vendor.

All servers and desktop, laptop, and workstation computers shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less. Employees shall log off their computers if they are going to be away from it for more than two hours. All tablet computers shall have an idle timed screen-lock secured with a six-digit PIN.

Because information contained on portable computers (e.g., laptops, tablets) is especially vulnerable, special care shall be exercised. At a minimum, the use of a unique password or PIN shall be used. Some data is extremely sensitive and employees are strongly encouraged to have multiple layers of protection on these files.

All postings by employees from a department email address to a newsgroup shall contain a disclaimer stating, "The opinions expressed are those of the author and not necessarily those of the department," unless they are posted in the course of business duties.

Using Data From an Outside Source

Employees shall use extreme caution when dealing with all email attachments, especially those received from unknown senders, or unexpected attachments from known senders. Emails frequently carry *malicious programs* that can easily, quickly, and irrevocably destroy or corrupt all data within a computer, server, or *networked system* and compromise the entire HPD computer network.

Employees shall use extreme caution when using any data brought in from an outside source. When outside data is used, employees shall first scan the files for *malicious programs* before downloading or using the information, even if the data comes from the employee's personal computer.

Employees shall use extreme caution when using USB drives (thumb drives) from unknown or untrusted sources. Simply inserting

a USB drive containing malicious software can easily, quickly, and irrevocably destroy or corrupt all data within a computer, server, or a *networked system* and compromise the entire HPD computer network.

4 UNACCEPTABLE USE OF COMPUTERS

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, or international law.

The following subsections include lists of prohibited activities that are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use of computers.

Prohibited Computer and Networked System Activities

Employees shall not:

a. Violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property laws, or similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" materials or other software products that are not appropriately licensed for use by the department.

b. Copy or use copyrighted material including, but not limited to, digitization and distribution of photographs, music, or literary works that are not authorized. This also includes the installation of any copyrighted software for which the department or the end user does not have an active license.

c. Export software, technical information, or encryption software or technology that is not authorized. The appropriate level of management shall be consulted prior to exporting any material in question.

d. Intentionally introduce *malicious programs* into the network or server.

e. Reveal their account password or PIN to others or allow the use of their account by others (see General Order 400-22, **Keys, Passwords, and Personal Identification Numbers**). This includes family and other household members when work is being done at home.

f. Use any department equipment to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws (see General Order 300-11, **Discrimination, Harassment, and Other Prohibited Conduct**).

g. Make fraudulent offers of products, items, or services originating from any department account.

h. Make statements about warranty, expressed or implied, unless it is within the scope of assigned duties.

i. Commit *security breaches* or *disruptions* of network communication, unless these duties are within the scope of assigned duties.

j. Conduct port scans or security scans unless otherwise authorized by the Office of Technology Services.

k. Execute any form of network monitoring that intercepts data not intended for the employee's host, unless it is within the scope of assigned duties.

l. Circumvent user authentication or security of any host, network, or account.

m. Interfere with or deny service to any user other than the employee's host (e.g., denial of service attack).

n. Use any program, script, or command, or send messages of any kind with the

intent to interfere with or disable a user's terminal session, via any means, locally or via the *networked system*.

o. Provide information about or a list of department employees to any party outside the department without the express direction of the Office of Public Affairs, Open Records Unit or other authorized department entity.

Personnel are reminded that criminal history checks are restricted to official police business. Employees are accountable for the correct use and dissemination of this information.

Prohibited Email and Communication Activities

There are no exceptions to these prohibited activities. Employees shall not:

a. Send junk mail, *spam*, or other advertising material including sales solicitations of any type to individuals who did not specifically request such material.

b. Harass any person (see General Order 300-11, **Discrimination, Harassment, and Other Prohibited Conduct**) via email, telephone, or any type of paging or communication device, whether through language, frequency, or size of messages.

c. Use or forge email header information that is not authorized.

d. Create or forward "chain letters" or "Ponzi" or other "pyramid" schemes of any type.

e. Solicit email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

f. Send from or through HPD's *network system* or any other service provider unsolicited email that advertises any group or service sponsored by the department.

g. Post or *spam* the same or similar non-business related messages to large numbers of Usenet newsgroups.

5 ENFORCEMENT

Any employee found intentionally violating this policy shall be subject to disciplinary, civil, or criminal actions.

6 RELATED GENERAL ORDERS AND REFERENCE MATERIAL

200-14, **Telephone Regulations**
300-11, **Discrimination, Harassment, and Other Prohibited Conduct**
400-11, **Paging Devices**
400-13, **Police Computer Systems**
400-14, **Control of Police Department Property**
400-18, **Responsibility for City Property**
400-19, **Microcomputer Regulations**
400-21, **Mobile Computing Devices**
400-22, **Keys, Passwords, and Personal Identification Numbers**
800-06, **CJIS Compliance**
800-09, **Official Document Archives**
800-10, **Police Records**
City of Houston Administrative Procedure (A.P.) 8-1, Use of City Information and City Information Technology Resources; and A.P. 8-2, Cybersecurity Program

Charles A. McClelland, Jr.
Chief of Police