General Order

Houston Police Department

ISSUE DATE:	NO.
May 17, 2022	400-13

REFERENCE: Supersedes all prior conflicting Circulars and Directives, and General Order 400-13, dated October 31, 2014

SUBJECT: ACCEPTABLE USE OF COMPUTER SYSTEMS

POLICY

Access to and use of the department's computer systems is strictly controlled. Except as provided by this General Order, all computers owned, leased, rented, or under the control of the department shall be used for business purposes in serving the interests of the city, and any data created (whether on- or off-site) on a department owned or controlled computer or computer system is the property of the department.

This General Order applies to all employees.

DEFINITIONS

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

Computer Systems. Databases and systems accessible by computers controlled by the department or to which the department has non-public access, including but not limited to the CAD system, records management system, Intranet Portal and associated programs (e.g., Police Personnel System), and various local, state, and federal databases approved for law enforcement use.

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

Spam. Unauthorized or unsolicited messages sent to a large number of recipients via the Internet or the act of sending such messages.

1 ACCEPTABLE USE OF COMPUTERS AND COMPUTER SYSTEMS

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

Much of the information obtained through a computer or computer system contains confidential and sensitive data that must be carefully controlled to ensure that the department is in compliance with applicable local, state, and federal guidelines and statutes. Employees shall only obtain, use, release, and/or disseminate criminal justice information from computer systems for legitimate law enforcement purposes. Security clearance and access to computer systems is restricted to official police business and does not permit an employee to access data for personal

reasons. Employees are reminded that criminal history checks are restricted to official police business, as required by General Order 800-06, **CJIS Compliance**.

Employees shall only obtain, use, release, and/or disseminate information about department administration, including information about employees gathered from any computer system, for legitimate and authorized administrative purposes. Employees shall not provide information about or a list of department employees to any party outside the department without the express direction of the Office of Planning & Data Governance, Open Records Unit, or other authorized department entity. All outside requests for information shall be carefully considered in light of the Open Records Act of the Texas Civil Statutes and departmental resources. When appropriate, such requests for information shall be directed to the proper authority, as required by General Order 800-10, **Police Records**.

Employees may use computers for personal reasons for a brief period, such as 3-5 minutes, to check the weather forecast or news sites. However, employees shall exercise good judgment regarding personal use.

Employees are reminded that all transactions performed over a computer or computer systems are logged for record-keeping purposes.

Prohibited Computer Activities

Employees shall not use a computer to:

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. The department purchases licenses for the use of software from a variety of outside companies. Employees shall use all software according to the applicable software license agreement.

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. Procure or transmit material that is in violation of sexual harassment or hostile workplace laws, or harass any person via email, telephone, or any type of paging or communication device, including through language, frequency, or size of messages, as prohibited by General Order 300-11, **Discrimination, Harassment, and Other Prohibited Conduct**.

f. Make fraudulent offers of products, items, or services originating from any department account, or make statements about warranty, expressed or implied, unless it is within the scope of assigned duties.

g. Commit security breaches such as accessing data the employee is not intended to receive, logging into a computer, server, or account the employee is not expressly authorized to access, or disrupting network communication through methods such as network sniffing, ping floods, packet spoofing, denial of service, and forged routing information, unless these activities are within the scope of assigned duties.

h. Conduct port scans or security scans unless authorized by the Office of Technology Services (OTS).

i. 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.

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

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

l. Send messages or use any program, script, or command of any kind with the intent to interfere with or disable a user's terminal session, via any means.

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

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

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

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

q. Send unsolicited email that advertises any group or service sponsored by the department.

r. Perform any action that would cause disruption of any MCD or cause interference with the reasonable supervision of officers.

Supervisors shall ensure department and City of Houston policies and procedures regarding computers and mobile devices are implemented and observed. All employees shall comply with all computer related policies, procedures, and software licensing agreements the department or City of Houston holds.

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 equipment on a periodic basis to ensure compliance with this policy.

2 USE OF INFORMATION FROM COMPUTER SYSTEMS

Employees shall not receive security access to any computer system unless authorized by the employee's division commander.

Authorized use of computer systems is restricted to:

a. Entering, modifying, or inquiring records in local, state, and national databases.

b. Dispatching.

c. Obtaining information necessary for the efficient and expeditious performance of the department's operations.

Information received from a computer system shall not be considered probable cause for arrest until it has been properly verified for accuracy. Information received through a computer system should be considered in conjunction with other information about the circumstances of an offense before any arrest decision is made.

When an incident report is flagged "Confidential" by an investigative division (e.g., Homicide, Narcotics), only the division that initiated the flag can authorize access to the report.

Confidential Status for Employee Information

The Crime Analysis & Command Center Division (Command Center) shall coordinate all requests for confidential status of employee information. Classified and civilian employees wanting their home address and telephone number to be confidential shall write a letter of justification via their assistant chief to the Command Center giving specific reasons for the request.

The following employees shall be prioritized for confidential status of employee information:

a. Officers who spend the majority of time serving as an undercover investigator, if access to the officer's home address or telephone number would endanger the officer or family members.

b. Officers who primarily investigate possible criminal violations committed by department personnel.

c. Employees who have received a personal or family-directed threat of death or serious bodily injury, if the employee's division commander and Criminal Intelligence Division personnel have determined that the threat is legitimate.

d. Employees who have a spouse with confidential status.

Employees not meeting any of the above guidelines may request an exception from the Chief of Police via the employee's chain of command. The request shall include details about the employee's duties and responsibilities and explain why there would be a high level of danger to the employee or family members if the home address or telephone number were accessible.

Employees shall provide justification for confidential status to the Command Center on an annual basis or it shall be removed. The Command Center shall distribute a quarterly list of employees with confidential status to each affected division for review and corrections. If an employee transfers, has a change of duties, or the situation posing a threat changes, the division commander where the confidential status originated shall write a letter to the Command Center to advise of the change. The employee's information shall then become readable in the computer system.

Command Center personnel have access to confidential address and telephone information at all times and can be contacted for emergency requests.

3 SECURITY AND PROPRIETARY INFORMATION

Any information accessed via computer systems 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 by any person, including all authorized personnel affiliated with third parties, as required by General Order 800-06, **CJIS Compliance**.

Each employee shall use a unique username and password to access a computer system. Employees shall keep passwords and personal identification numbers (PINs) secure and shall not share accounts, as required by 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 computer systems, 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 OTS 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 other computers and mobile devices shall have an idle timed screen-lock secured with a unique password or six-digit PIN.

Employees who forget their HPD Windows password should contact their division technology coordinator to get it reset. If the technology coordinator is not available, the employee should contact the Service Desk for OTS. A Service Desk employee shall initiate a process to confirm the employee's active status and reset the employee's password to a temporary password. At the earliest opportunity, the employee shall change the temporary password to something known only to the employee. Once the employee's password has been reset by the technology coordinator or the Service Desk, the employee may go to the "Password Enrollment" link on the department's Intranet Portal to enroll in the HPD Password Self-Service feature.

NOTE: The HPD Password Self-Service feature can be used to reset or unlock only an employee's HPD Windows password. Once enrolled, employees will be able to reset or unlock their own Windows password by clicking on the "*Need help with your password?*" link on the Windows log-in screen of any computer connected to the HPD computer network.

Because information contained on computers and mobile devices is especially vulnerable, employees shall exercise special care when using such equipment. Some data is extremely sensitive and employees should have multiple layers of protection on such data.

All postings by employees from a department email address to an external forum 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 Outside Sources

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 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 a computer system and compromise the entire HPD computer network.

Employees shall use extreme caution when using USB drives (thumb drives). Simply inserting a USB drive containing malicious programs can easily, quickly, and irrevocably destroy or corrupt all data within a computer, server, or a computer system and compromise the entire HPD computer network.

4 USAGE OF MOBILE COMPUTING DEVICES AND LAPTOPS

The MCD system shall be used to aid in the dispatching and servicing of calls for service while reducing the amount of voice radio usage. Emergency Communications Division personnel shall use voice communications as the primary assignment medium in all instances in which an officer's safety would be best served by having other field personnel aware of the officer's location and assignment. Follow-up information may be transmitted over the MCD system, as permitted by General Order 600-01, **Response Management**. Field personnel shall use an MCD, if so equipped, to maintain their unit status in a timely and proper fashion.

All officers assigned and trained in the use of laptop computers or MCDs shall use the laptop or a suitable MCD for incident report entry whenever possible. Any employee encountering problems with the approval of an incident report shall contact the Service Desk.

Troy Finner
Chief of Police