

General Order

Houston Police Department



ISSUE DATE:

October 31, 2014

NO.

400-13

REFERENCE: Supersedes all prior conflicting Circulars and Directives, and General Order 400-13, dated October 13, 1994

SUBJECT: POLICE COMPUTER SYSTEMS

POLICY

This General Order establishes a set of strict guidelines for governing access to and use of the department's centralized computer systems.

This General Order applies to all employees.

1 AUTHORIZATION AND USE

Authorized use of centralized police computer systems is restricted to the following:

- a. Entries, modifications, and inquiries on local, state, and national computers.
- b. Dispatching.
- c. Prisoner bonding.
- d. Information necessary for the efficient and expeditious performance of the department's operations.

The centralized police computer systems are intended solely as an aid to employees in the performance of their assigned responsibilities. Employees shall limit their system activities to those necessary to accomplish their assigned responsibilities. Security clearance and access to information is restricted to official police business and does not permit any employee access to information for personal reasons.

2 USE OF INFORMATION

Much of the information available through the centralized police computer systems

contains confidential and sensitive data that must be carefully controlled to ensure the department is in compliance with applicable local, state, and federal guidelines. Any employee accessing police files or obtaining information from a centralized police system shall be held accountable for the appropriate and correct use of the information and for the proper disposal of the information.

Information obtained through the computer shall not be considered probable cause to arrest. Information received through the computer should be considered in conjunction with other information about the circumstances of an offense before any arrest decision is made.

3 SECURITY

Based on the nature of their duties, most classified personnel shall be granted access to computerized police information, including, but not limited to, incident reports and general name and personnel inquiries. However, 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. Civilian employees shall not receive security access to any police information system unless authorized by the employee's division commander.

Each employee who uses a personal computer, laptop, or mobile device to access centralized police systems shall be held accountable for its proper operation and shall be responsible for each transaction made. Each employee shall use a unique user name and password to access a police computer system. Employees shall not reveal

their user name or password or allow anyone else to use those credentials to gain access to any HPD computer system.

Employees who forget their Windows (computer) password must contact their division technology coordinator to get it reset. If the technology coordinator is not available the employee should contact the Service Desk for HPD's Office of Technology Services. 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 sign on to the centralized computer system and 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 (computer) password. Once enrolled, employees will be able to reset or unlock their own Windows (computer) 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.

4 CONFIDENTIAL STATUS FOR EMPLOYEE INFORMATION

The Command Center is responsible for coordinating all requests for confidential status of employee information. Classified and civilian employees wanting their home address and telephone number confidential must write a letter of justification via their assistant chief to the Command Center giving specific reasons for the request.

The following guidelines shall be used as a basis for granting confidential status of employee information:

- a. When an officer spends the majority of time serving as an undercover investigator and access to the officer's home address or telephone number would endanger the officer or family members.
- b. Internal affairs 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 and 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.
- e. **EXCEPTIONS:** 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 must provide 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 have to provide justification for confidential status 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 them 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.

Employees are reminded that this information is not to be released without proper authority (General Order 800-02, **Media Relations**).

5 RESPONSIBILITY

The Office of Technology Services is responsible for monitoring and managing all HPD personal computers, laptops, and mobile devices that access centralized police computer systems and for maintaining the integrity of HPD's computer network and related systems.

6 RELOCATING EQUIPMENT

Any division or section planning to relocate shall notify the Office of Technology Services in order to effect the safe and proper movement of computer equipment. Such notifications shall be given as soon as possible to avoid unnecessary delays or interruptions in computer service. Equipment shall be moved only by those persons designated by the Office of Technology Services. Under no circumstances shall any other employee move any HPD owned computer equipment.

7 REPORTING EQUIPMENT PROBLEMS

Any problems encountered with HPD computer equipment should be immediately reported to that division's technology coordinator. If the problem cannot be resolved, the Service Desk for the Office of Technology Services should be contacted.

8 ABUSE OF EQUIPMENT

Employees operating a police computer system shall exercise reasonable care of the equipment. Employees shall be held responsible for any damage resulting from intentional abuse or negligence (e.g., spilled drinks or food, paper clips).

9 RELATED GENERAL ORDERS

- 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 and Passwords**
- 400-25, **Acceptable Use of Computers**
- 800-02, **Media Relations**
- 800-06, **CJIS Compliance**



Charles A. McClelland, Jr.
Chief of Police