



SUBJECT
COMPUTER PROCEDURES

NUMBER
402/52

EFFECTIVE DATE:

08-26-09

AMENDS:

08-12-08


RESCINDS:

DISTRIBUTION: Administration, CID, Patrol, Communications, Clerical

REFERENCES:

**CALEA 41.3.7, 82.1.7 / IACLEA 82.1.7
TPCFA 9.07.1**

- .10 PURPOSE:** The purpose of this directive is to establish Departmental policy and procedures concerning the use of Alamo Colleges and Police Department in house networked, stand alone and mobile computer hardware and software.
- .11** Under no circumstances shall a procedure established herein, or the interpretation thereof compromise Officer Safety in any way.
- .20** Instructions in this procedure apply to all Department members unless the context or specific language indicates limited applicability.
- .21** The use of Department networked, stand alone and mobile computers will be limited to those operations that support the Department's mission.
- .22** Members shall not utilize or access Alamo Colleges computers not assigned to the Police Department.
- .30 MOBILE/FIELD USAGE: OFFICERS' RESPONSIBILITIES:**
- A. The driver of any vehicle equipped with a mobile data computer shall not operate the computer while the vehicle is in motion. Solo – officers assigned portable computers will stop their vehicle and park in a safe manner before attempting to access information.
 - B. Officers assigned an MDT are required to use the MDT to make all CJIS/TCIC/NCIC inquiries unless circumstances exist that make using the MDT impractical.
 - C. The responses from inquiries to the CJIS/TCIC/NCIC systems are protected information. Officers are not permitted to use these systems for their own use and information received through these computer systems may only be used for official criminal justice purposes.
 - D. Officers shall not initiate any inquiry outside those purposes necessary to complete a Departmental objective. Officers shall also ensure that unauthorized persons do not view responses from these systems.

	<u>SUBJECT</u> COMPUTER PROCEDURES		<u>NUMBER</u> 402/52
	EFFECTIVE DATE: 08-26-09	AMENDS: 08-12-08	RESCINDS:
DISTRIBUTION: Administration, CID, Patrol, Communications, Clerical		REFERENCES: CALEA 41.3.7, 82.1.7 / IACLEA 82.1.7 TPCFA 9.07.1	


E. Food and drinks shall not be allowed in any vehicle equipped with an MDT.

.40 ELECTRONIC MESSAGING PROCEDURES:

- A. Electronic messages sent on the Department's computer systems will be for Department business purposes only.
- B. Short personal messages are allowed as long as they are not offensive or embarrassing to the Department in any way.
- C. The mobile data computer message logs may be periodically reviewed at the direction of the Chief of Police or his/her designee to assure proper procedures are being followed.
- D. Members are reminded that any electronic message that is sent through the mobile computer system may later be retrieved, even though it may have been deleted from the assigned employee's computer.
- E. Members are reminded that electronic messages are not a protected form of communication and could be subject to a discovery motion in a criminal case, civil case, or internal investigation.
- F. Every electronic message should be considered to be in the public domain.
- G. Assigned employees have no expectation of privacy regarding electronic messages.
- H. All electronic messages should be professional and courteous.

.41 SECURITY/STORAGE:

- A. Only the District's Information Technologies Department is authorized to work on, repair, replace parts, relocate or install software on Department computers.
- B. It shall be the assigned employee's responsibility to safeguard the computer using every precaution available (i.e.; locking their vehicle when left unattended in the

	<u>SUBJECT</u> COMPUTER PROCEDURES		<u>NUMBER</u> 402/52
	EFFECTIVE DATE: 08-26-09	AMENDS: 08-12-08	RESCINDS:
DISTRIBUTION: Administration, CID, Patrol, Communications, Clerical		REFERENCES: CALEA 41.3.7, 82.1.7 / IACLEA 82.1.7 TPCFA 9.07.1	

case of MDT's, securing computers in the office by password protection, etc. in the case of desktops).

- C. Any use of a Department computer by anyone other than an authorized user is prohibited.
- D. It shall be the assigned employee's responsibility to ensure the security of the computer against unauthorized use.
- E. Employees will not give their passwords to any other person or persons to use, nor will they leave the password in any discernible written form in or near their computer.
- F. Assigned employees, however, may be required to disclose this information to someone in their chain of command or support personnel for departmental business purposes.
- G. All employees are required to log off from all network computer systems at the completion of their workday.
- H. The District's Information Technologies Department must be notified if Department computers or peripheral equipment are damaged, stolen, in need of repair or it is believed unauthorized access was attempted or gained.

.50 MAINTENANCE:

- A. The District's Information Technologies Department is responsible for all maintenance, support and repair of Department computers.
- B. Requests for service should be routed to the Deputy Chief of Administration on the designated form.
- C. In an effort to assist the District's Information Technologies Department in resolving computer problems, the person reporting should make every effort to document the nature of the problem with specific detail of the problem.



SUBJECT
COMPUTER PROCEDURES

NUMBER
402/52

EFFECTIVE DATE:
08-26-09

AMENDS:
08-12-08

RESCINDS:

**DISTRIBUTION: Administration, CID, Patrol,
Communications, Clerical**

**REFERENCES:
CALEA 41.3.7, 82.1.7 / IACLEA 82.1.7
TPCFA 9.07.1**

- D. With the knowledge and at the direction of the District's Information Technologies Department, other personnel may perform minor maintenance on Department computers. This minor maintenance does not alter the need for security or installation approval from the District's Information Technologies Department.
- E. All software installations shall be coordinated with the District's Information Technologies Department to ensure compatibility and that it is virus free.

.60 TRAINING:

- A. It will be the responsibility of the assigned employee to maintain Texas Crime Information Center (TCIC) certification, if required by the employee's supervisor or specific job assignment.
- B. It will be the responsibility of a member's supervisor to schedule additional computer training specific to the software available to the assigned employee if needed.