

USE OF COMPUTERS AND PERIPHERAL EQUIPMENT

This order establishes policies and procedures governing the use of computers and the confidentiality of computer data.

I. POLICY

The policy of the Department is to protect all confidential information from unauthorized disclosure and access and require responsible use of all computers, electronic mail and the Internet.

II. PROCEDURES

A. USERNAMES AND PASSWORDS

1. All access to computer use and the data contained within is protected by the use of individual user names and passwords issued to a member by the Department. No member shall access any Department computer for any purpose by using a user name and password other than those issued to the member by the Department.
2. Members shall maintain the confidentiality of their Department-issued user name and password. Members shall not disclose their username and password to any other person with the following exceptions:
 - a. Authorized members of the M.I.S. Unit
 - b. Upon the request of an officer conducting an administrative investigation
 - c. Pursuant to an order from the Chief of Police.
3. Members shall be responsible for all computer access logged under their user name and password.
4. If a member forgets his or her user name and/or password, the member shall request a new user name and/or password by submitting a memorandum through the chain of command to the Deputy Chief of Administration. When the Deputy Chief of Administration approves the request, the MIS Unit will issue a new user name and/or password to the member.

DGO 10.08

03/29/02

B. ISSUANCE OF DEPARTMENT EQUIPMENT

1. The Deputy Chief of Administration through the MIS Unit shall authorize the distribution of all computers owned or controlled by the Department. This includes computers obtained through purchase, donation, seizure, forfeiture, unclaimed property, and grants.
2. A member requesting any computer equipment (hardware or software) shall forward a memorandum through the chain of command to the Deputy Chief of Administration. The memo shall include the member's reason for requesting the equipment and any known or potential funding source.
3. No member shall modify any Department computer equipment or install any device or program, including but not limited to any peripherals such as external storage devices, printers, scanners or any type of communication device without written approval of the Deputy Chief of Administration.

C. USE OF PERSONALLY OWNED COMPUTERS.

1. A member who requests permission to use a personally owned computer for Department purposes shall submit a memorandum through the chain of command to the Deputy Chief of Administration. The memo shall include the make(s), model number(s) and serial number(s) of all hardware components and the manufacturer(s) title(s), version number(s) of all software loaded on or that may be loaded on the computer.
2. Members shall not use software obtained in violation of copyright laws.
3. The Department shall not be responsible for the repair, maintenance or upgrade to personally owned computer hardware or software. Any damage to personal property shall be governed by DGO 3.15.

D. UNAUTHORIZED USE OF OFFICE TECHNOLOGIES

1. Members may use Department owned and issued equipment, including computer equipment, for work related purposes only.
2. No member shall use access to e-mail, the Internet, or any computer program for any purpose other than those reasonably necessary for the performance of his or her work assignment. (Penal Code § 502). Members are specifically prohibited from using e-mail or Internet accounts to access information reasonably considered offensive or disruptive to any member. Offensive content includes, but is not limited to, sexual comments or images, racial slurs, gender-specific comments, or any comments that would reasonably offend someone on the basis of age, sexual orientation, religious or

political beliefs, national origins or disability.

3. Only the MIS Unit may create, administer and maintain e-mail or Internet accounts on Department owned or issued computers, and may do so only with the approval of the Deputy Chief of Administration. Any member requesting an e-mail or Internet account shall do so by submitting a memorandum through the chain of command to the Deputy Chief of Administration.
4. No member shall access any criminal history information except as necessary for a bona fide criminal investigation. No member shall access computer history information for curiosity, personal or political purposes. All members accessing confidential criminal history information shall be familiar with Department rules and regulations and local, state and federal laws regarding proper access and use of such information.

E. PRIVACY OF COMPUTER INFORMATION. Members shall not have an expectation of privacy for information stored or accessed through Department owned or issued computer equipment. Authorized Department personnel may access information stored or contained on any Department computer, and may log and monitor network activity, without notice at any time. This includes monitoring and logging Internet and e-mail use. Members shall not create any unauthorized security barriers to the Department's access to their computers or files.

F. DISSEMINATION OF INFORMATION THROUGH THE INTERNET

1. **THE DEPARTMENT'S OFFICIAL WEBSITE.** The City's Department of Telecommunications and Information Services (DTIS) administers the Department's official Web Site. Any member requesting the addition of any information to the Department's Web Site shall submit the request by memorandum through the chain of command to the Deputy Chief of Administration. If approved by the Deputy Chief of Administration, the MIS Unit will submit the request to DTIS.
2. **HOME PAGES AND OTHER INTERNET SERVICES.** No Member shall convey official Department information, or make any representation, actual or implied, that he or she is conveying official Department information on any web site or in any other form through the Internet, other than through the Official Department Web Site, except with the express written permission of the Deputy Chief of Administration.

G. RESPONSIBILITIES OF THE MANAGEMENT INFORMATION SERVICES (M.I.S.) UNIT.

The M.I.S. Unit shall be responsible for:

1. Acquiring, installing, repairing, maintaining and replacing all Department owned or

DGO 10.08
03/29/02

issued computer hardware and software, including peripherals.

2. Arranging and managing all computer support/maintenance agreements.
 3. Registering all computer hardware and software and shall be the Registered Licensee.
 4. Inspecting and auditing all Department computer equipment.
-