

MAUI COUNTY POLICE DEPARTMENT

GENERAL ORDERS
CHAPTER 308
COMPUTER OPERATIONS

Effective date: 8/18/20

Revision date: 7/08/20

Rescinds: GO 308.1 (5/01/06)

New materials underscored

Accreditation Standards: 11.4.4, 82.1.6

INFORMATION TECHNOLOGY AND SECURITY
G.O. 308.1

I. PURPOSE

The purpose of this order is to provide guidelines to Department employees in order to ensure the agency's computer system and computer equipment remains secure.

II. POLICY

This policy applies to all equipment that processes, stores, and/or transmits NCIC Criminal Justice Information, classified and sensitive data, and media that is owned or leased by the Maui Police Department, including the Records Management System. Maui Police Department employees will ensure all computer use and electronic communications conform to Department policy as well as local, state and federal laws.

III. PROCEDURES

A. System Security Access

1. Each computer user is provided with a unique user ID and password(s) to access various Departmental computer programs and databases. User IDs and passwords establish accountability for actions performed, and all actions performed are the responsibility of the person who has been assigned that user ID.
 - a. No user may sign on to any computer or program using another person's password.
 - b. Users shall ensure that unauthorized persons do not learn their passwords. In the event that a user suspects their password has been compromised, he or she shall immediately notify the Quality Assurance Section.
 - c. Users who have gained access to a confidential database or other restricted programs shall not leave their terminals unattended or unobserved without first signing off. It is the responsibility of the user to ensure that his or her password does not provide an unauthorized person with access to a restricted program or file.

2. The Quality Assurance Section is responsible for overseeing the Records Management System to ensure user IDs and passwords are valid as well as ensuring no system access violations occur.
- B. Annual Security Audit
1. Annually, the Quality Assurance Section or designee, will audit user names and passwords used to access Maui Police Department applications.
 - a. This audit will compare a listing of current employees to a listing of authorized passwords and user names.
 - b. User names and passwords not assigned to current employees will be disabled.
- C. Computer System Usage
1. The Department provides computer information systems for the purpose of conducting official business and as permitted, some personal use. This technology enhances productivity and effectiveness. However, abuses of the Department's computer systems may result in disciplinary action.
 2. The primary criterion in the matters of use or misuse of computer systems will be that of reasonableness. While there are specific unauthorized uses, the Department recognizes the reality of the workplace and allows limited personal use of the systems.
 3. The Department, as the employer, retains the right to determine what is and is not appropriate for the workplace. Access to the computer information systems is a privilege, and not a right. All use of these systems shall be in a professional manner consistent with best business practices, the Department's General Orders, and local, state, and federal laws.
- D. Restricted Access to Specific Material/Sites
1. Employees are not allowed to access or enter pornographic sites, sites that display nudity or partial nudity, or any other sites that a reasonable person would know is inappropriate in the workplace.
 2. Other types of use that are not permitted are the viewing, downloading or uploading of profanity, racially or culturally biased material, disparaging comments or images of an ethnic nature or that disparage a specific gender, and/or accessing/sending materials involving the use of harassing language, images, jokes, or messages that disparage any person, group, or classification of individuals whether or not a recipient consented to or requested such material

3. Employees that must access such sites for legitimate investigative purposes shall report their use at the soonest available opportunity to their supervisor.

E. Limited Personal Use

1. Employees may access the computer information systems, such as the Internet, for personal reasons on-duty while on their authorized work breaks.
2. Personal use must not interfere with the employee's duties and responsibilities, or the duties and responsibilities of any other employee.
3. Personal use must not incur liability or costs to the Department.
4. Personal use shall not be of such a nature that it brings disrepute to the Department or its employees.

IV. SOFTWARE

- A. To prevent computer viruses from being transmitted through the department's computer system, downloading of any unauthorized software is strictly prohibited. Only software registered through Maui Police Department may be downloaded.
- B. Manipulation or alteration of current software on Mobile Data Computers (MDC) installed in patrol cars is restricted from users without local administrator's access on the MDC.

V. STORAGE

- A. Only work related data files are allowed on shared network drive(s).
- B. The amount of storage of work related data on the shared network drive can be limited at the operational discretion of the Information Technology Section.
- C. Storage of pornographic material is prohibited on shared network drives.
- D. Files will be reviewed and may be deleted 90 days after separation.
- E. Employees are prohibited from deleting work related material upon transfer or separation.

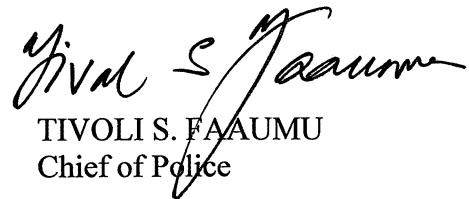
VI. INFORMATION TECHNOLOGY SUPPORT

- A. The Quality Assurance Section will coordinate support for applications that manage classified and sensitive data to include:

1. Criminal Justice Information Services

2. National Crime Information Center
3. Juvenile Justice Information System
4. Open Fox
5. Live Scan
6. Computer Aided Dispatch
7. Hawaii Integrated Justice Information System
8. Records Management System
9. Body Worn Camera System

B. The purchase of computers and related equipment shall be made via channels to the Office of the Chief.


TIVOLI S. FAAUMU
Chief of Police