FREDERICK POLICE DEPARTMENT
GENERAL ORDER

Section 9: Police Equipment and Vehicles
Order Number: 975
Topic: AUTOMATED INFORMATION SYSTEM (AIS)
Issued by: Chief of Police
Approved: 06/06/2017
Review: Annually in October by Commander, TSD
Supersedes: G.O. 975 dated 03/03/16

.01 PURPOSE:

To describe the Department's policy, procedures, and guidelines relating to the proper use of personal computers, and related electronic messaging systems, including the Criminal Justice Information System (CJIS) devices utilized by the Department for purposes of disseminating electronic mail, utilizing services of the Internet and related electronic message transmission, recording and storage devices and accessing sensitive law enforcement criminal justice information

.02 CROSS-REF:

G.O. 978, "Mobile Data Terminal System"
CALEA Standards: 82.1.6

.03 DISCUSSION:

The availability and use of the personal computer within the work environment has provided many opportunities for enhancement of productivity and effectiveness. These technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this Department, its members, and the public if not managed properly.

.04 POLICY:

It is the policy of this Department that use of its computer technology be strictly limited to the official business of the Frederick Police Department, and that its members strictly adhere to all state and federal regulations that govern the dissemination of law enforcement and/or confidential information. All members will abide by the guidelines set forth herein when using personal computers and the services of both internal and external databases and information exchange networks, and where applicable, voice mail, mobile data terminals (MDTs) and related electronic messaging devices. No employee will have any expectation of privacy with regard to any information on the computer systems. The Department reserves the right to monitor messages, inspect mail and review transactions occurring on AIS.

.05 DEFINITIONS:

AUTOMATED INFORMATION SYSTEM (AIS) – The computer hardware, software, and infrastructure that make up the Department's information/data system. For purposes of this Order, AIS includes personal computers, electronic mail systems, voice mail systems, smart phones, tablets, paging systems, electronic bulletin boards, Internet services, MDTs, and facsimile transmissions.

INTERAGENCY INFORMATION TECHNOLOGIES (IIT) – The electronic communications equipment and services provided by Frederick County Government (FCG).

.10 REQUIREMENTS PERTAINING TO VOICE MAIL AND ELECTRONIC MAIL:

The Department has provided to certain individuals voice mail and electronic mail to increase the proficiency of their assigned duties and to provide greater access to members by the public and professional colleagues. Members having voice mail and electronic mail will follow the requirements listed below:

1. Members are expected to become proficient in voice mail and electronic mail equipment assigned to them, and they are to utilize the equipment to enhance their professionalism and efficiency. Personnel will ensure that they complete "housekeeping" duties to ensure electronic mailboxes, voice mailboxes do not become overloaded to prevent them from receiving messages. All sworn members of the Department will be issued a smart phone device. With the exception of Command level personnel, this will be the sworn members only voice mail option. Command level personnel will be provided a County voice mail extension in addition to their Department issued smart phone device.

2. Members are required to access their voice mail every working day. Members subpoenaed for off-duty court will follow procedures in Section .40 of G.O. 1401 pertaining to voice mail.

   A. Voice mail announcements will be created and modified to reflect availability of the member and when the caller can expect messages to be returned. Accordingly, announcements will be modified when members are on vacation, utilizing compensatory leave, or on absences from regularly assigned duties (for example, for more than one week). Modified outgoing voicemail messages will identify when the member will return to duty and shall indentify alternate agency personnel who may be contacted during the absence of the member. The outgoing voicemail message shall include the telephone number of the alternate personnel covering for the absent member.

   B. Members will respond back to all voice mail messages promptly upon receipt unless there are extenuating circumstances.

3. Members are required to access their electronic mail on a frequent basis, as prescribed by their division commander, and respond promptly to any messages/requests made by others.

   A. Automated "Out of Office" email announcements will be created and activated to reflect when members are on vacation, utilizing compensatory leave, or on absences from regularly assigned duties (for example, for more than one week). Automated Out of Office email responses will identify when the member will return to duty and shall indentify alternate agency personnel who may be contacted during the absence of the member. The automated email notification message shall include the email address and agency telephone number of the alternate personnel covering for the absent member.

   B. Personnel will utilize e-mail in lieu of paper copies of documents whenever feasible for such items as notifications of meetings, drafts of general orders, requests for information, etc.

   C. E-mail will not be utilized for formal documents that require hand written signatures as proof of receipt.

4. Members who access their Department e-mail on either Department-issued or personally-owned smart phones or tablets must ensure the automatic screen lock feature is enabled, activates within one minute or less if the phone is not used, and is deactivated only by a pass code, PIN, password, pattern, or fingerprint. Furthermore, **any** data device with access to Department e-mail must never be sold, transferred, exchanged, or otherwise given to any non-FPD entity, including employees of wireless service providers (Verizon, AT&T, et.al.) unless the Department e-mail account and any other stored, sensitive information has been deleted. A breach of law enforcement sensitive information from an unsecured Department-issued or personally-owned smart phone or tablet because of a failure to comply with the security measures in this paragraph may

result in disciplinary action.

.15 GENERAL:

1. The computer hardware which comprises the Department's AIS is a network of desktop computers, MDTs, lap top computers, printers and scanners, which are linked together in a local area network (LAN) which is supported by an infrastructure maintained by IIT under a formal, written agreement with the Department.

2. All computer hardware used by the Department needs to be able to be integrated into the LAN unless there is a specific reason to require "stand alone" capability; therefore, the Commander, TSD, will review and authorize all future computer hardware requests/orders prior to purchase.

3. Only the Commander, TSD, the IT Manager, or his designee, is authorized to modify, repair, adjust or otherwise change the configuration or set-up of any AIS component including the movement or relocation of any AIS component.

4. All software used in AIS is licensed and registered to the Frederick Police Department or Frederick County Government, is intended for the official business use of the Department, and is protected by federal copyright law. Personnel are expressly prohibited from using any unlicensed, copied, or "pirated" software programs on any departmental computer for any purpose; removing or copying any AIS software for any purpose; and installing any software program on any departmental computer without the written authorization of the Commander, TSD. Only the Commander, TSD, the IT Manager, or his designee, is authorized to purchase, install, modify, or remove software programs from AIS. Any violation of the hardware/software restrictions may result in administrative action as well as criminal prosecution for violation of the copyright laws or licensing agreements.

5. The Commander, TSD will be responsible for the secure storage of all single user software purchased by the Department for use on its computers.

6. The agency Terminal Agency Coordinator (TAC) will be responsible for installation of CJIS applications.

7. All sworn members of the Department, as well as select non-sworn members of the Department will be issued a smart phone device in order to increase operational efficiency and effectiveness. All personnel will maintain strict adherence to the guidelines outlined in this order when using the device. There is no requirement or expectation while in an off duty status that members check electronic mail or voice mail. Personnel who are in an on-call status will be subject to re-call as outlined in G.O. 1210 (Manpower Availability).

.20 AIS RESTRICTIONS:

1. Transmission of electronic messages and information on communications media provided for members of this Department will be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence or public records.

2. AIS and its contents are under the control of the Frederick Police Department and are intended for use in conducting official business. Members are advised that they do not maintain any right to privacy in AIS equipment or is contents.

3. The Department reserves the right to access any of the records within the system at any time and to retain or dispose of those records as it deems necessary and appropriate and

may require members to provide passwords to files that have been encrypted or password protected.

4. The Department reserves the right to access, for quality control purposes and/or for violation of this policy, data, electronic and voice transmission of members conducting business of the Department.

5. Accessing or transmitting materials (other than that required for police business) that involves the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage the Department, any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

6. Confidential, proprietary, or sensitive information may be disseminated only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained. When possible, such information should be made available through shared directories or networked systems. If it is necessary and lawful to store and/or disseminate confidential, proprietary, or sensitive information on removable storage media such as CDs, DVDs or USB flash drives, the employee in rightful possession of the media is responsible for its physical security. Such information includes, but is not limited to, the following:

   A. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information;

   B. Confidential informant master files, identification files, or related information; and,

   C. Intelligence files and information containing sensitive tactical and undercover information.

7. No member will access or allow others to access any file or database, including CJIS, unless that person has a need and a right to such information. Additionally, personal identification and access codes will not be revealed to any unauthorized source. Personnel will not remain logged into a workstation if it will be unattended for any length of time. Once a user is logged onto the computer system, they are responsible for any transactions that occur under the log-on identification and password.

8. Members will not download or install on their personal computer or network terminal any software or other materials from the Internet or other external sources without taking prescribed steps to preclude infection by computer viruses. Material will be downloaded to a storage media and scanned for viruses prior to being entered into any personal or shared system only after receiving permission of the Commander, TSD. In no case will external materials or applications be downloaded directly to any shared (network) drive. When in doubt, members will consult the Commander, TSD or the IT Manager for guidance.

   A. Occasionally personnel may use their own personal computer or another computer outside AIS to complete a report or project. Because of the consequences an imported virus may have on AIS, all personnel are prohibited from using any storage media which has been used on a computer outside AIS until it has been scanned for a virus.

   B. Modems may also introduce a virus into AIS; therefore only modems authorized by the Commander, TSD, or the IT Manager, will be used for AIS.

C. In the event a user suspects that a virus is affecting the AIS, he will immediately notify the Commander, TSD, or the IT Manager, who will initiate a virus scan.

9. AIS is designed and intended to conduct business of the Department and is restricted to that purpose. Installation of, or access to, software for purely entertainment purposes is prohibited. Exceptions to business use include the following:

A. Infrequent personal use of these devices may be permissible if limited in scope and frequency. The use must be in conformance with other elements of this order and not connected with a profit-making business enterprise or the promotion of any product, service, or cause that has not received prior approval of this agency. This policy does not permit use of printing devices for personal use.

B. Personnel may make off-duty personal use of agency computers for professional and career development purposes when in keeping with other provisions of this policy and with prior knowledge of an appropriate supervisor.

.25 INTERNET INFORMATION CONCERNING THE DEPARTMENT:

1. The Department has an official web page on the Internet. The web page is maintained by the IT Department for the City of Frederick. The staff of the Office of the Chief of Police is responsible for coordination and minor changes of content of the web page (excluding press releases). He/she will be responsible for periodically reviewing and updating the information contained on the web site to ensure the information is current. Any member who wishes to include information on the web site will forward the information to the OCP and/or TSD, via the chain of command, for inclusion, if appropriate.

2. Creating a web site on the Internet that has any appearance of officially representing the City of Frederick or the Frederick Police Department is prohibited without the express written approval of the Chief of Police.

3. Using scanned images of any official Department logo, patch, or badge on personal web pages is prohibited without the express written approval of the Chief of Police.

.30 FREDERICK COUNTY TECHNOLOGY USE POLICY:

1. The Department is permitted to utilize the infrastructure of the electronic communications system of Frederick County. All personnel must abide by the County's regulations concerning the system as well as the Department's regulations. (Where noted in this section, "County" will also apply to members of the Department.) The County's electronic communications systems are the property of the Frederick County government and are intended for use in carrying out government business. The "Frederick County Technology Use Policy" states, in part:

> The electronic communications systems are the property of FCG and are intended for use in carrying out government business. FCG reserves the right to monitor the operation of its electronic communications systems, to access all of the records within them, to retain or dispose of those records, and to disclose the contents of those records as it deems necessary. FCG retains all personal property rights in any matter created by FCG users or paid to be created with FCG funds, unless explicitly stated otherwise in FCG approved contracts.
>
> System users of FCG's electronic communications systems cannot be guaranteed privacy, nor should there be an expectation of privacy. System users must not assume privacy just because a private password is used. The use of passwords to gain access to the electronic communications systems is for the

protection of FCG, not its users. Electronic communications are “official records” under the Maryland Public Information Act and are potentially subject to disclosure. Although access to information and information technology is essential to the missions of government agencies and their users, *use of electronic communications systems is a revocable privilege.* Conformance with acceptable use, as expressed in this policy statement, is required. The system user’s division will enforce this policy with the assistance of IIT, and may further restrict technology use.

2. The County designates the following “Specifically Acceptable Uses”:

   A. Communication and information exchange directly related to the mission or work tasks of the system user’s division;

   B. Communication and information exchange for professional development, to keep current with training or education, or to discuss issues related to the user’s division activities;

   C. Applying for or administering grants or contracts for governmental research or programs;

   D. For advising, distribution of standards, research, analysis and professional society activities related to governmental work tasks and duties;

   E. Announcement of new laws, procedures, policies, rules, services, programs, information or activities; and

   F. Public wireless access is provided as a service for the public to access the Internet in FCG office buildings. Private wired and wireless access is provided for approved and supported FCG devices.

3. The County designates the following “Specifically Unacceptable Uses”:

   A. Purposes that violate the laws of the U.S. or the State of Maryland or the laws, rules, regulations or policies of FGC or its divisions and agencies, as applicable;

   B. For-profit, commercial, charitable or public service activities, unless sponsored by the system user’s division and approved by the division’s director;

   C. The intentional copying of any software, electronic file, program or data using FGC provided electronic communication services without a prior, good faith determination that such copying is, in fact, permissible. Efforts to obtain permission from the owner of such information should be adequately documented;

   D. System users intentionally representing themselves electronically as others, either on FGC networks or elsewhere unless explicitly authorized by the user’s division director and IIT. System users shall not circumvent established policies defining eligibility for access to information, networks or systems, or circumvent established monitoring procedures;

   E. Intentionally developing and/or executing programs to infiltrate a computer, computing system, or communications network and/or damage or alter the software components of same unless authorized by IIT;

   F. Use that is not consistent with all applicable laws or policies prohibiting

discrimination, harassment, obscenity, libel, political activity, and the marketing of products and services;

G. Creating any messages that would be offensive to a reasonable person or would be disruptive. Remotely accessing IIT supported computers without the full knowledge and approval of IIT; and.

H. Connecting a non-IIT supported computer to FGC private wired or wireless networks without the full knowledge and approval of IIT.

4. The County designates the following "System User Responsibilities":

A. System users are expected to use electronic communications systems responsibly and professionally and shall make no intentional use of these resources for any unlawful purpose.

B. System users must not violate personnel policies, procedures or codes of conduct while using FGC electronic communications system.

C. System users share in the responsibility for system security. Authorized system users must use passwords to gain access to the network and applications. The choice of passwords should not be so obvious that others could easily guess them. System user's passwords must not be shared with other users. If any user suspects that their password has been compromised, they are to notify their supervisor and IIT, and change the password as soon as possible. Procedures for choosing good passwords and changing passwords can be obtained by contacting IIT.

D. System users shall use the network judiciously and promote efficient use of the network to minimize congestion, which might interfere with the work of other employees. For example, accessing Internet sites for large file downloads or to provide continuous streaming media consumes a significant amount of essential resources (bandwidth), which affects the performance of the network and its users. Examples of streaming media are internet radio, music, television, training videos, and presentations. Although these are prohibited for personal use… some of these can be a very critical part of the work process, but should be disconnected as soon as it is no longer needed.

E. System users must observe existing copyright, licensing, and legal restrictions on the use of software or information.

F. Internet access through the FCG network shall be strictly limited to that which is necessary to conduct governmental-related business, except as noted in the Personal Use section of this document.

.35 CARE, MAINTENANCE, AND PHYSICAL SECURITY OF HARDWARE:

1. Personnel will exercise common sense and good judgment when operating computer equipment so as to protect and to preserve the hardware. Food, drink, etc. should not be placed in proximity to computer hardware that can be damaged by an accidental spill.

2. Power surge protectors have been installed on every device. These devices will not be removed from the computers except upon the authorization of the IT Manager.

3. In the event any hardware is damaged, the employee who discovers or is responsible for the damage will notify the Commander, TSD, in writing via chain of command, detailing to the best of his/her knowledge of how the damage occurred. Personnel are prohibited

from attempting to adjust, modify, or repair any AIS hardware for any reason.

4. In the event any hardware is malfunctioning, the employee who encounters the malfunction shall notify TSD at his/her earliest opportunity by submitting an electronic FPD HelpDesk request for repair. If essential work cannot be performed without the equipment, a call may be made to the TSD Commander to expedite the repair. Personnel are prohibited from attempting to adjust, modify, or repair any AIS hardware for any reason.

5. Laptop computers or computer notebooks need to be in the physical possession of the user or locked in the trunk of the departmental vehicle. When not assigned for departmental use to a specific individual, these devices will be secured in a locked cabinet or locked desk as designated by the Commander assigned control of the device. In the event a lap top computer is lost or stolen, the user will immediately notify the on-duty supervisor who will begin an immediate investigation into the incident.

6. The Commander, TSD or IT Manager is solely responsible for the proper disposal of any AIS equipment/component. Disks, USB flash drives, magnetic tapes, cassettes, etc., that contain or may have contained sensitive/confidential information will be forwarded to the Commander, TSD, for proper disposal if they are not being reformatted or reused. The Commander, TSD will ensure that any hardware that may contain or may have contained sensitive/confidential information is cleared of that data prior to delivery to a service representative.

.40 MANAGEMENT OF THE AUTOMATED INFORMATION SYSTEM:

1. The responsibility for the overall management and technical support of AIS rests with the Commander, TSD. He will:

   A. Provide daily management/technical support for AIS by coordinating services with the Interagency Information Technologies (IIT), Frederick County when appropriate;

   B. Monitor the use of AIS for compliance with established departmental policy and procedures as well as state and federal laws and regulations, and revise as necessary;

   C. Develop and coordinate all AIS training programs to include the certification and recertification of all personnel who access to the CJIS/NCIC/MILES function;

   D. Maintain current license agreement records for all software used by AIS;

   E. Perform periodic AIS audits and inspections as directed by the Chief of Police;

   F. Review, coordinate, and/or prepare all budget requests for computer hardware and software;

   G. Oversee the acquisition and installation of all hard and/or software obtained by the Department;

   H. Modify existing AIS equipment as needed; and,

   I. Ensure adequate computer file space for current records through management of available file space as per existing law and/or procedure.

2. The IT Manager will provide backup support to the Commander, TSD, in his absence. The Commander may appoint, as required, additional backup support personnel

necessary to support automation efforts.

3. All agency personnel are assigned a login and password to access computer systems. Access rights and abilities are assigned to each person depending on their specific job requirements. The Commander, TSD, or IT Manager are responsible for determining computer access rights assigned to each login and password and coordinating issuance of login and passwords by the proper authority.

4. Annually, during the month of August, the TSD Commander or IT Manager will audit system logins, verifying valid logins for each required employee. Conversely, the IT Manager will ensure the termination of system access immediately for each employee upon ending employment with the Department.

5. The Department's core automated systems consist of the following; computer aided dispatch (CAD), records management system (RMS) and our local area network (LAN) for traditional office automation. These systems are maintained by Frederick County – Interagency Information Technologies (IIT). IIT conducts disc to disc backups of all systems to an offsite location. Backups are run at least nightly, while others take place throughout the day.