POLICE DEPARTMENT
HANOVER PARK, ILLINOIS

DIRECTIVE: 507-S

REFERENCE STANDARDS: 41.3.7 82.1.7 82.1.9

SUBJECT: Information Systems

PURPOSE: The Hanover Park Police Department utilizes a variety of computer systems in providing services to the community. Employees shall be trained in the use of various computer systems that is related to their specific assignment and shall exercise the utmost level of integrity with all computers, local networks, and non-local networks. Computerized networks include, but not limited to, the Law Enforcement Agencies Data System (L.E.A.D.S.), DuPage County Criminal Justice Information System (CJIS), DuPage Communications E-911 and Mobile Data Terminals (MDT), Village of Hanover Park Network Management System governed by the Village of Hanover Park Electronic Communications Policy, and the Internet.

I. DEFINITIONS

Application Password - a password that a user may assign within an application that prohibits other users from opening the secured application.

Hardware - Computer components that include, but are not limited to, processor, keyboard, monitor, printer, mouse, cables, connectors, adapters, telephones, and any other device attached to any component.

Network - System of connected devices (computers, printers, etc.) that communicate and share services.

Network Password - a code usually consisting of alpha and numeric characters that a user utilizes to gain access to a network.

Personal Computer (PC) - a stand-alone computer system.

Personally Owned Laptop – a laptop computer owned by the employee and authorized to use for Village of Hanover Park business.

Power on Password - a password assigned to the hardware of a PC that prevents other users from starting the system.

Software - Any removable magnetic media, diskette, CD, or program that resides on or can be copied to removable magnetic media for use in or written in a computer readable language.

System Administrator - The individual responsible for operating and maintaining the department's computer network system.

Workstation - Desktop or Laptop computer that is connected to the network. Workstations give the user access to network services.

II. PROCEDURES

A. LEGAL OBLIGATIONS

1. Use of an electronic computer is subject to all federal, state, and local law, including, but not limited to:
   a. Illinois Compiled Statutes concerning computer crime.
   b. Illinois Compiled Statutes concerning pornography and related offenses.

2. Personally owned laptop computers, when used for Village business, are subject to the same policies.

B. SUPERVISOR RESPONSIBILITY

1. Makes request to Data Processing Division for employee accounts, training, and certification.

2. Has authorization, through the Deputy Chief of Support Services, to request access to employee files from Data Processing Division, in the absence of the employee, that require an immediate response or action. This may occur when the employee's supervisor has knowledge of an important assignment being handled by the employee and circumstances require immediate file access.

3. Provides Data Processing employees' access to workstations for routine maintenance, loading software or reconfiguring.
   a. Should unauthorized hardware or software be located on employer provided equipment, Data Processing Division employees have the authority to remove such equipment or software after notification of the supervisor of that workstation.
      1) Unauthorized hardware or software includes all equipment or programs not purchased or licensed by the village.
   b. Discovery of unauthorized hardware or software at a workstation shall be documented by the supervisor and sent to the Deputy Chief of Support Services.

4. Supplies input towards the purchase and installation of new or revised hardware through the Data Processing Division to assure the continued preservation of the system's integrity.

6. Coordinates the movement, disconnection or disassembly of computer components (computers, printers, modems, etc.) through the Data Processing Division.

7. Reviews files relevant to employee assignments that need revision or purging. Authorizes the purging of files in coordination with other department supervisors (when files are used by other department employees) and the Data Processing Division.

8. Authorizes the use of a personally owned laptop computer for Village business through the Deputy Chief of Support Services.
   a. Ensures employees authorized to use a personally owned laptop for Village business read and sign a waiver regarding their and Village's obligations.
      1) A waiver shall be signed for each laptop authorized. (Appendix A)
   b. Confirms that backup disks of Village business on personally owned laptops are current and accessible at all times.

9. The Data Processing Manager or his designee shall be responsible for maintaining an inventory of all Department computer hardware and software.

C. EMPLOYEE RESPONSIBILITY

1. Toward local and non-local networks.
   a. Be knowledgeable of the policy and operations manuals related to all computer systems used.
   b. Be knowledgeable of other computer related policies, such as Electronic Communications.

2. Internet activity.
   a. Use of the Internet will be governed by IV. Of this Directive.
   b. Discretion should be used when downloading of files from the Internet. A number of sites available on the Internet such as Bulletin Boards may contain computer viruses.
      1) All downloading of files from the Internet should be to the user's local hard drive (C: Drive) or to a diskette.
      2) Downloaded files are to be scanned for computer viruses prior to transferring to any network.
      3) Should viruses be detected the Data Processing Division should be notified immediately.

3. Before using a personally owned laptop computer, employees shall secure authorization from the Deputy Chief of Support Services and sign a waiver. (Appendix A)
    a. Adhere to all laws, policies and merit rules that apply to use of personally owned laptops when used for Village business.
    b. Provide supervisor current backup files of Village business stored on personally owned laptop.

4. Exercise caution to protect the system's integrity.
    a. Exercise a high level of security with remote accounts and direct access accounts or from a stationary workstation within the department.
    b. Upon activating the account the employee selects a unique password to gain future access to the account, per the systems policy.
        1) Passwords do not entitle the employee to a sense of privacy. The department may engage in monitoring of electronic files created by employees for valid purposes, including employee supervision. This applies to personally owned computers when used for Village business.
    c. Employees shall not disclose their password to others or attempt to obtain other persons' passwords.
    d. Log out of the system when absent from the workstation so as not to create a security hazard.
    e. Routinely reviews files for purging of old or unneeded files they created for their use only.

5. Exercises caution to protect the system's physical well being.
    a. Installing or deleting of software on employer owned equipment is prohibited unless directed by the Data Processing Division.
    b. Movement, disconnecting or disassembling of computer components (computer, printer, modem, etc.) from workstations is prohibited unless directed by the supervisor through the Data Processing Division.
    c. Coordinate through the supervisor and report to the Data Processing Division all equipment that is malfunctioning.
    d. Maintain workstation clean and free of dust and dirt.
    e. Keep food, liquid, and other harmful articles away from computer workstations.
    f. Exercise the same high level of physical security for laptops and other portable computer components as with other department computer equipment.

D. SOFTWARE USAGE (82.1.7)

1. Computer software generally is a licensed product. The Village purchases the right to use a computer program on a specified number of workstations. The department respects all computer software copyrights and adheres to the terms of software licenses.

a. Employees shall not duplicate any licensed software obtained for the department's use.
b. Shareware software is also copyrighted material that is distributed free for a trial period. Should the department or employee have a qualified use of a shareware program those programs shall also be licensed.
c. Employees personally owned/licensed software shall not be installed on Village owned equipment.

E. RESTRICTIONS (82.1.9)

1. Use of any PC or workstation for any purpose that violates any federal, state, or local laws is prohibited.

2. Personal use of Police Department network computer workstations is discouraged. However, there may be legitimate uses for the network involving work that is reasonably relevant to the organizational mission, and is therefore authorized once approval is obtained from the Deputy Chief of Support Services.
   a. Personal use of LEADS, NCIC, intelligence, or local file databases is strictly prohibited. Unauthorized use of such databases will be met with disciplinary action and, in some cases, may result in criminal prosecution.

3. Use of any PC or workstation for commercial purposes or for material gain while on or off duty is prohibited.

4. Sending harassing, intimidating, abusive or offensive material to or about others is prohibited.

5. Using another person's identity and another person's password is prohibited.

6. Employees shall not add, remove, or reconfigure employer owned computer components without approval of the supervisor through the Data Processing Division. This includes hardware and software.

7. Employees experiencing system network problems shall not shut off the PC or workstation until the appropriate system administrator has been contacted.

8. The use of Passwords shall only be used with supervisory permission and be on file with supervisors and accessible by system administrator representatives.

9. Unplugging workstations from surge protectors is prohibited.

10. No software shall be added, deleted or in any way modified in the CAD terminals. All such requests or needs shall be routed to the CAD System Administrator in the Emergency Communications Department at DuComm.

III. MOBILE DATA TERMINALS (41.3.7)

All Mobile Data Terminals (MDT's) used by the Hanover Park Police Department are subject to the rules and regulations of multiple entities to include, but not limited to, the Federal Communications Commission (FCC), DuPage Public Safety Communications (DuComm), the Illinois Law Enforcement Agencies Data System (LEADS), and various other Federal, State, Local and Departmental laws, rules, regulations and guidelines.

MDT's are computers that operate through the use of radio frequencies and are thus radio transmitters and receivers under the control of the FCC. All MDT's operated by the Hanover Park Police Department are done so through DuPage Public Safety Communications (DuComm). All department MDT's are capable of accessing various forms of protected information to include that governed by LEADS policy and State and Federal laws such as wanted information, and various other protected personal information.

A. Approved Uses of MDT System

1. Routine drivers license, vehicle registration, and wanted/stolen inquires.

2. Routine work related messages.

3. Status Changes.

4. Anything of a "**sensitive**" nature, i.e.: specially indicated information about an address or person, communicating while on a "stake out", or anything of such a nature that it should not be broadcast over the radio.

B. Prohibited Acts

In addition to the potential violations of State and Federal law, it shall also be violation of Department policy to:

1. Disclose any information accessed via MDT to any person other than law enforcement members and only then when said officer is acting in his official capacity for an authorized law enforcement function.

2. Utilize the MDT for anything other than an official law enforcement necessity.

3. Utilize the MDT in such a manner as to otherwise violate any other applicable rule or regulation.

4. Signing on to an MDT using another members code or using an MDT while said MDT is signed on by a member other than the member accessing the MDT.

C. Prohibited Messages

1. Officers shall utilize verbal radio transmission policies, procedures and standards in their use of MDT messaging. Utilization of MDT messaging capabilities for personal information exchange and critical information transmission that merit appropriate documentation on verbal transmission frequencies are strictly prohibited.
2. Messages from MDT's to DuComm advising status changes, clearance codes or activity will not be accepted or acted upon solely by them. Officers are still expected to change status, clear calls and advise their activity via DuComm radio.

D. Accountability

The Deputy Chief of Support Services or his designee shall conduct periodic inspections of transmissions stored in computer databases to insure compliance with the caveats of this order.

Due to the nature of MDT transmissions, all messages are logged to a disc file at DuComm. Messages are stored for a period to time before erasing. Printouts of all messages sent from a particular terminal or by a particular officer or telecommunicator are available to Department and DuComm Staff personnel upon request. DuComm telecommunicators and Department personnel are therefore cautioned to be prudent and judicious in using the MDT system. Failure to comply with the provisions of this directive may result in disciplinary action.

IV. INTERNET ACCESS

A. Personnel will have access to the Internet provided via the Village of Hanover Park network system after the Chief of Police gives authorization. Violations of any of the rules regarding Internet use will result in the elimination of the offending member's Internet access and appropriate disciplinary action.

B. Business, unacceptable use, privacy and security measures governing Internet use are outlined in the Village of Hanover Park's Electronic Communications Policy and will be adhered to.

C. Electronic Mail (E-Mail)

1. The Chief of Police may authorize E-Mail access to members through a coordinated effort with the Village's Data Processing Department in accordance with policies through that division. Violations of E-Mail access rules will result in the elimination of E-Mail access by the offending member as well as appropriate disciplinary actions.

2. E-Mail may be used for the following purposes:
   a. Department activities and/or correspondence;
   b. Personal activities and/or correspondence within reason and so long as all appropriate rules are followed;
   c. Courtesy correspondence for Village staff; or
   d. Other correspondence as assigned.

3. E-Mail **will not** be used for or in the following manner:
   a. The posting of any correspondence deemed inappropriate to include, but not limited to, material containing references of a sexually explicit or implicit nature, profane or vulgar language, language of a racist nature or derogatory to persons based on race, sex, ethnicity or sexual orientation;
   b. For purposes of commerce, secondary employment or solicitation;
   c. Any use other than for a legitimate business related purpose of the Hanover Park Police Department;
   d. Any other manner that may be deemed inappropriate.

4. Responsibilities to check for E-Mail
   a. Members who have an assigned E-Mail address will check for incoming messages at the beginning of each workday (at a minimum). Additionally, it is suggested that E-Mail boxes be checked on a regular basis based on anticipated volume of incoming E-Mail.

5. E-Mail is the property of the Village of Hanover Park and its Police Department.
   a. Any E-Mail (including personal) constitutes an official Police document. It is subject to inspection at any time. This material is fully discoverable by most courts in addition to internal inquiries.

V. ATTACHMENTS

A. Village of Hanover Park Employee Acknowledgment Receipt of Electronic Communications Policy. (Appendix B)

VILLAGE OF HANOVER PARK

EMPLOYEE ACKNOWLEDGMENT

RECEIPT OF ELECTRONIC COMMUNICATIONS POLICY

This certifies that I have received a copy of the ***Electronic Communications*** policy approved by the Village President and Board of Trustees on February 17, 2000. I agree to read and become familiar with its contents.

I understand that this policy is subject to change at the discretion of the Village Manager and that I may ask any supervisor or department head for an explanation or for further information on this policy.

_____ _____

Employee Signature *Date*

Original: Personnel File
Copy: Retain in Employee's Copy of Manual

HANOVER PARK POLICE DEPARTMENT

LAPTOP COMPUTER WAIVER

For the mutual convenience of the Village of Hanover Park and me, I am being allowed to use my personally owned laptop computer, described below, while on Village business. As a part of this agreement, I understand the following:

1) The retention of any personal data or information in my personally owned laptop computer is at my own risk and the Village of Hanover Park will not be responsible for any loss.

2) My personally owned laptop computer, described below, is subject to entry, search, and inspection by my superiors without further notice.

3) Any privately owned property contained in my personally owned laptop computer might be opened and examined without further notice or without my permission. Therefore, I have no expectation of privacy when using my personally owned laptop computer for Village business.

4) The obligations that apply to employer-provided computer equipment, including all laws, policies, and personnel rules, apply to my personally owned laptop computer when I use it for Village business.

5) I understand that the Village is not responsible for any maintenance on my personally owned laptop computer while I am using it for Village business.

6) The Village is not responsible for any loss I may incur as a result of using my personally owned laptop computer for Village business.

7) A current backup disk file will be maintained of all Village business and accessible to my supervisor.

8) Either party may terminate this agreement at any time.

Computer Description:

Computer Brand: _____

Computer Serial Number: _____

_____ _____

D/C Support Services Signature Employee Signature

Date: _____ Date: _____

Appendix A; DIR 507-S