


| | | |
|---|---|---|
| NORTHAMPTON POLICE DEPARTMENT | |  |
| Administration & Operations Manual | | |
| Policy: Management Information Systems and Computer Use | | AOM: S-110 |
| Massachusetts Police Accreditation Standards Referenced: [82.14.1b], [11.5.1], [82.1.1], [82.1.2], [82.1.7], 82.1.1.a, [82.1.6] | | Issuing Authority <hr/> John Cartledge Chief of Police |
| Dissemination Date: 05/25/2000 Effective Date: 06/08/2000 | Amended: 6/02, 7/04, 8/05, 8/06, 2/07, 9/08, 11/08, 1/09, 1/12, 5/13, 7/13, 2/14, 1/18, 2/22 Reviewed: 6/02, 7/04, 8/05, 1/07, 9/08, 11/08, 1/09, 1/12, 5/13, 2/14, 3/16, 1/18, 1/19, 10/20*, 10/21, 2/22, 10/23, 4/26 | |

Contents

| | |
|----------------------------------|---|
| I. Introductory Discussion | 1 |
| II. Policy | 1 |
| III. Procedures | 2 |

I. Introductory Discussion

This directive describes the Northampton Police Department’s guidelines with regard to employee access to and disclosure of information contained on the Department’s computer system, including incident and criminal information on the CJIS server systems, wireless system laptops in police cruisers, and electronic mail messages and information contained on the shared network.

II. Policy

It is the policy of the Northampton Police Department to maintain a management information system in order to provide reliable information to be used in performing its required functions and duties, as well as in management decision-making.

The information is important for analyzing work load, determining resource needs, budget preparation, resource allocation, record keeping, employee safety and other departmental needs. Access to data contained in the system must be controlled in a manner that will ensure only authorized access.

It is also necessary to permit dissemination of public data to interested individuals. This data must be in conformance with the Criminal Offenders Records Information (CORI) laws and the standards of the Massachusetts Criminal Systems History Board in order that the rights of any individual are not infringed. All information needs to be carefully reviewed prior to dissemination to ensure that it is not restricted.

III. Procedures

A. Administration: The information system provides a comprehensive representation of the department's operation at any given point in time, as well as projecting future trends from current and past data.

1. Responsibility for recording and/or providing specific types of data is assigned to and/or shared by various shifts or bureaus. Types of data recorded into the system include, but is not limited to the following (list modified to alpha):

- a. Alarms
- b. Arrest bookings
- c. Business directory
- d. Calls for service
- e. Collision data
- f. Department inventory
- g. Digital photos
- h. Emergency notification list
- i. Employee attendance
- j. Evidence
- k. Field interviews
- l. Incident report narratives
- m. Intelligence Records
- n. Juveniles
- o. Master names
- p. Motor vehicle citations
- q. NIBRS
- r. Offender history
- s. Policing trends
- t. Restraining orders
- u. Stolen property
- v. Street files
- w. Tows
- x. Trespass lists
- y. Vehicles

B. Records: All incident reports, arrests, summons, motor vehicle violations, criminal offender histories, and various other records are entered into the

Department computer system and are assigned a unique and sequential case number. These records may be accessed by Departmental personnel from any network computer, and are available 24 hours a day. [82.1.1,b] [11.4.4]

1. **Juvenile Records:** Offender histories for juveniles will be segregated electronically from adults. Digital records will be marked with the word “*Juvenile*” in red at the top of the report. Juvenile records will be maintained as such after an individual has become an adult. [82.1.1] [82.1.2]
2. **Release of Records:** Members of the public requesting access to department records shall be referred to a member of the Records Bureau. Records Bureau Personnel will disseminate records in accordance with the state public records law and with the CORI Act (refer to *AOM S200,tb1 Criminal Offender Record Information*). All information must be carefully reviewed prior to dissemination to ensure that it is not restricted. [82.1.7] [82.1.2][11.4.4]

C. Equipment, Hardware, Software and Systems:

1. **Adding/Modifying/Transferring Software & Hardware (including on-line sources):** Requests for adding/modifying/transferring software and/or hardware shall be submitted to the IT department via the helpdesk system. No one may add or modify software or hardware to computers under the control of this Department without the authorization of the Chief of Police. [11.5.1]
2. **Licensing:** All programs introduced into the system shall be properly licensed.

D. Password/Computer Access/Security: Software and hardware have been installed to prevent unauthorized network access. The System Administrator(s) will assign access codes (logins) and the initial user’s passwords for the department computer network system and RMS software: [82.1.1,a]

1. Users will change the initial password every ninety (90) days when prompted at log in. Passwords are encrypted and are known only to the users.
2. Users may not divulge their passwords to anyone without the authority of the System Administrator(s).
3. Users shall not utilize passwords issued to other persons to access the department computer system without the authority of the Chief of Police or System Administrator(s).
4. Access codes will be audited to verify all logins.
5. Logins will be audited annually for verification of all passwords, access codes and access violations. [82.1.1]
6. Logins no longer needed shall be disabled on the system server.
7. Generic Admin accounts shall be removed.

E. Computer File Backup & Storage: On premise backups are stored on a Datto Appliance which is located in the Dispatch Data Center. Our on premise backups replicate to an off-premise cloud storage location managed by our vendor, Total

Communications who are responsible for ensuring everything is functioning as expected on a day to day basis.

Colocation protects us from types of cyberattacks (ransomware etc.) and gives us disaster recovery protection (fire, flood etc.) All backups of servers containing sensitive data (IMC/DHQ etc.) are fully encrypted, both on and off premise.
[82.1.6]

1. On-premise backups are retained for 2 months, cloud backups are retained indefinitely.
 2. Matters of policy (retention time, backup frequency etc.) are set the IT Director.
- F. Use of Department E-Mail & External Internet Services: All internal e-mail messages whether sent or received by employees and all files located or accessed by departmental computers are considered department records. All external files, including personal e-mails and data that are accessed using departmental computers are not considered private communications, and can be subject to scrutiny and/or disclosure by proper departmental or legal authority.
1. Personal Use of Department Computer System: Because the Northampton Police Department provides e-mail, Internet, and computer systems to assist employees in the performance of their duties, employees should only use it for official Department business. Occasional personal use of the e-mail, Internet and computer system is permitted if the use:
 - a. Does not consume more than a trivial amount of time and resources that could otherwise be used for business purposes.
 - b. Does not interfere with user productivity.
 - c. Does not preempt any department-business activity.
 - d. Is not for any purposes that will produce personal financial gains.
 - e. Is not for the distribution or printing of copyrighted materials (including articles and software) violating copyright laws.
 - f. Is not for sending, receiving, printing, or otherwise distributing proprietary data or other confidential information.
 - g. Is not for sending, voluntarily receiving, or soliciting offensive, improper, or harassing statements or language including disparagement of others based upon their race, marital status, national origin, sex, sexual orientation, age, disability, religious, or political beliefs.
 - h. Is not for sending, voluntarily receiving, or soliciting sexually oriented messages or images.
 - i. Is not used for sending chain letters, gambling, or engaging in any other activity which violates the law.
- G. Physical Security of the Server Room & Electronic Media:
1. The Server Room/Data Center, like all areas that are non-public areas shall be secured at all times. Only authorized personnel shall have access to the Server Room/Data Center and that access shall be recorded by the Department's

Access Control System. Unauthorized persons needing to have access to the Server Room/Data Center shall be escorted at all times.

2. Electronic Media consists of both Internal and External Hard Drives, Removable Media (such as DVDs, CDs, Thumb Drives, Zip Disks, Floppy Disks, etc.) and other technology storage devices. Electronic Media shall be stored in appropriate secure locations.
- H. Only System Administrators shall have the authority to access the computer system remotely. System Administrators shall only use the means of remote access that require both an initial authentication and a secondary type of authentication in addition to regular NPD network credentials.
1. The Chief of Police and the Captains shall have the authority to access their computer remotely to conduct departmental business. The Chief of Police and Captains shall only use the means of remote access that require both an initial authentication and a secondary type of authentication in addition to regular NPD network credentials.
 2. The Court Administrator shall have the authority to access their assigned computer from the court during their working hours. The Court Administrator shall only use the means of remote access that require both an initial authentication and a secondary type of authentication in addition to regular NPD network credentials.

I. Sanitation and Disposal of Electronic Media:

1. Sanitation of Electronic Media Procedure: Format and/or overwrite the electronic media a minimum of three (3) times or by electronically degaussing.
 - a. Usable internal and external hard drives and removable electronic media no longer used shall be sanitized.
2. Disposal of Electronic Media Procedure:
 - a. Unusable internal and external hard drives and electronic media that cannot be sanitized shall be disposed of properly. Usable electronic media already sanitized that will no longer be used shall also be disposed of properly.
 - b. All electronic media destruction services shall be outsourced to a certified third party vendor.
 - c. Electronic media slated for destruction shall be placed in a secure case and locked by IT personnel prior to being transported to the secure destruction facility.
 - d. The physical destruction of the media shall be witnessed and attested to by CJIS-certified IT personnel.
 - e. Certificates of destruction shall be obtained from the ITAD vendor and retained by the IT department. Certificates shall include, at a minimum, the serial number of the destroyed asset and the date of destruction.