LAW ENFORCEMENT COMPUTERS

Shared Municipal and Police Computer Systems

Issued June 2000

TO: All County Prosecutors
Colonel Carson Dunbar, Superintendent, New Jersey State Police
All Chief Law Enforcement Officers

FROM: John J. Farmer, Jr., Attorney General

SUBJECT: Guidelines – Shared Municipal and Police Computer Systems

DATE: June14, 2000

1. Introduction

The Division of Criminal Justice has received increasing numbers of inquiries from police departments asking whether records may be placed on a computer system shared by the police department and non-law enforcement municipal agencies. While there are no statutes prohibiting the sharing of computer systems, the law provides many instances in which information that police departments gather is required to be kept confidential. Often, it is a disorderly persons offense to wrongfully disclose statutorily protected information.

As a result of these restrictions, most information stored on a police department computer system will need to be stored on a separate computer system that is not shared with non-law enforcement municipal agencies. However, personnel information may be kept on shared systems. Detailed guidelines are set forth in the body of this directive.

2. Scope of Application

These guidelines apply to information maintained by individual police departments. They are not intended to apply to terminal access to dedicated state or federal law enforcement data systems managed by the State Police. These systems are already governed by user agreements limiting system access. These guidelines do not supersede existing law enforcement data systems user agreements.

3. Examples of Confidential Police Records

The following table contains examples of Police records that must remain confidential:

Examples of Confidential Police Records	
Abuse of Institutionalized Elderly	*N.J.S.A.* 52:27G-13 – provides that it is a disorderly persons offense to disclose confidential information developed during an Ombudsman investigation.
Autopsy and Medical Examiner Reports	*N.J.A.C.* 13:49-3.1 – may only be disclosed by County Prosecutor or Attorney General once a death is referred for criminal investigation.
Child Abuse and Child Sexual Assault Victims.	*N.J.S.A.* 2A:82:46a – the name, address and identity of a victim under the age of 18 shall not appear on the indictment, complaint or any other public record. *N.J.S.A.* 2A:82-46b – it is a disorderly persons offense to disclose a report containing a child victim's name, address or identity. *N.J.S.A.* 9:6-8.10a – requires that all DYFS reports released to law enforcement be kept confidential.
Criminal Investigation Records	Executive Orders 123 and 69 – provide that these records are not subject to public disclosure.
Domestic Violence	*N.J.S.A*. 2C:25-33 – provides all records maintained pursuant to this act shall be confidential and shall not be made available to any individual or institution except as otherwise provided by law.
Electronic Surveillance	*N.J.S.A.* 2A:156A-19 – provides that it is a third-degree crime to knowingly use or disclose the existence of an intercept order or the contents of an intercept, except as authorized by statute or court order.
Grand Jury Information	*Rule* 3:6-7 – provides that Grand Jury proceedings are secret.*N.J.S.A.* 2B:21-10 – provides that any person who, with the intent to injure another, makes an unauthorized disclosure of Grand Jury information commits a fourth degree crime.
Internal Affairs Investigations	Attorney General's Internal Affairs Policy and Procedures – provides that contents of internal investigation case files are confidential. (*Law Enforcement Guidelines* page 11-20.)

Juvenile Delinquency	*N.J.S.A.* 2A:4A-60a – records pertaining to juveniles charged as a delinquent shall be strictly safeguarded from public inspection. *N.J.S.A.* 2A:4A-60h – disclosure is a disorderly persons offense
Juvenile-Family Crisis (Runaways, Truancy, etc.)	*N.J.S.A.* 2A:4A-60a – records pertaining to juveniles found to be part of a juvenile-family crisis shall be strictly safeguarded from public inspection. *N.J.S.A.* 2A:4A-60h – disclosure is a disorderly persons offense
Search Warrants	Court Rule *R.* 3:5-4 – provides that it is contempt of court to disclose the existence or basis for a search warrant prior to execution.

Of course, shared Criminal Justice Information Systems such as those operated by the Federal Government, the State Police and others also require that participants adhere to strict confidentiality standards, but these systems are beyond the scope of this directive.

4. Fundamental Principle

Police records do not acquire a new legal status as a result of being stored on a computer network. Confidential information may appear in many forms on the network. Word processing documents, E-mail, database or spreadsheet files may all contain confidential information. All information on police data systems must be maintained in such a way that non-law enforcement personnel do not have access to any information that they would not be permitted to see in a hard copy file. However, this restriction does not limit access to police computer files by clerical or other civilian police employees who must use police records in order to perform their duties.

5. Records Permitted to be Shared

Employment records that do not contain any confidential information may be shared with non-law enforcement municipal government agencies. Examples of such records include payroll records, name, title, and salary. In fact, New Jersey Department of Personnel regulations provide that certain records, such as an individual's name, title, salary, compensation, dates of government service and reason for separation are public. *N.J.A.C.* 4A:1-2.2a(1). Records containing such information may be placed on a shared server physically or remotely accessible by non-police personnel, except for routine maintenance or repair. However, care should be taken that confidential information regarding internal affairs investigations, or a law enforcement officer's role in an investigation, does not appear in any shared files.

6. Protected Information

Information related to any of the topics listed below, whether stored on computers or in physical files, shall not be accessible by non-police personnel, except upon court order, or to comply with the requirements of a statute, regulation or executive order:

- Arrests
- Autopsy and Medical Examiner reports
- Criminal Investigations
- Criminal History Records
- Criminal or Gang Intelligence
- Domestic Violence
- DYFS Reports
- Electronic Surveillance
- Evidence Receipts and Inventories
- Grand Jury
- Incident Reports
- Internal Affairs
- Juvenile Delinquency or Juvenile-Family Crisis
- Medical Reports
- Search Warrants and Affidavits

Police computer networks containing such information shall be controlled by a dedicated server, not physically or remotely accessible by non-police personnel, except for routine maintenance or repair.

7. Technical Support Services

It is understood that the network technical support staff for the system has the greatest level of access to the system and will be able to overcome any security barriers within the system and grant access to system users. The technical support staff persons are, therefore, in a position of great trust, and consideration should be given to having such staff work for the law enforcement agency, providing technical support to outside agencies as needed.

If technical support staff persons are employed by a non-law enforcement agency, someone within the agency must be designated to supervise the functions performed by the support staff. At a minimum, the law enforcement supervisor should maintain a current list of all users and their level of system access.

8. Background Checks for Technical Support Staff

If employed by the law enforcement agency, or a non-law enforcement agency, a background investigation must be conducted on all technical support staff hired after the effective date of this memorandum. This does not apply to private contractors employed for short-term purposes such as to perform installations or repairs.

The investigation will include completed state and federal applicant fingerprint cards submitted to the State Bureau of Identification (SBI). The employing agency must check the following state and national arrest and fugitive files prior to the submission of state and federal applicant fingerprint cards.

- New Jersey Computerized Criminal History (NJCCH)New Jersey Wanted Person System (NJWPS)
- NCIC Interstate Identification Index (III)
- NCIC Wanted Person File
- National Law Enforcement Telecommunication System (NLETS) Criminal History Record Information (CHRI) for non III participant states

If a record of any kind is found, pursuant to the remote terminal checks listed above, access to the law enforcement system shall not be granted, pending further investigative review and positive identification by both FBI and SBI fingerprint comparison. If the applicant is confirmed to be a fugitive from justice or has been convicted of an indictable offense, the applicant shall not be permitted to provide technical support services to a law enforcement computer system. Disorderly persons convictions shall not be an absolute bar to employment in this capacity, but access shall be denied by the law enforcement agency if it is determined not to be in the public interest.

9. Conclusion

As a result of these restrictions, most information stored on a police department computer system will need to be stored on a separate computer system that is not shared with non-law enforcement municipal agencies. However, personnel information may be kept on a shared systems.

Your cooperation in this matter is greatly appreciated. Kindly direct any questions on this issue to Thomas J. Fisken, Deputy Attorney General, Prosecutors and Police Bureau, at (609) 984-2814.