

	ELGIN POLICE DEPARTMENT 151 Douglas Avenue Elgin, Illinois 60120	
Effective Date: 11/29/17	STANDARD OPERATING PROCEDURE	Revised Date:
Chief of Police: 	Criminal Justice Information (CJI), 41.12	
Cross Reference:		Policy Sections: 41.12.1 Media Storage and Access 41.12.2 Media Sanitation and/or Disposal 41.12.3 Breach Notification and Incident Reporting

PURPOSE

The purpose of this policy is to establish guidelines for the protection and confidentiality of criminal justice information.

POLICY STATEMENT

It is the policy of the Elgin Police Department to maintain criminal justice information in a secure, professional, and confidential manner. Authorized personnel shall protect and control electronic and physical criminal justice information while at rest and in transit. The department will take appropriate safeguards for protecting criminal justice information to limit potential mishandling or loss while being stored, accessed, or transported.

DEFINITIONS

Criminal Justice Information: Any data which is a component of the Criminal Justice Information System to include, but is not limited to: Law Enforcement Agencies Data System (LEADS), National Crime Information Center (NCIC), Criminal Query History (CQH), and Secretary of State data bases.

Electronic Media: Memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Physical Media: Includes printed documents and imagery that contain criminal justice information.

PROCEDURES

41.12.1 MEDIA STORAGE AND ACCESS

Controls shall be in place to safeguard electronic and physical media containing criminal justice information, hereinafter referred to as CJI, while at rest, stored, or actively being accessed. To protect CJI, authorized personnel shall:

- A. Utilize secure passwords for access to all data systems. Passwords shall be complex and not be dictionary words or other words or numbers that would be easily linked to the owner.
- B. Passwords shall not be shared with anyone else including ITS personnel. Passwords shall never be sent over email to anyone.
- C. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
- D. Restrict access to electronic and physical media to authorized individuals.
- E. Ensure that only authorized users remove printed or digital media from any CJI system.

- F. Physically protect CJI electronic media until the end of its life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. Refer to Section 41.12.2 to view information on electronic media sanitation and disposal.
- G. Store all physical media in a secure area, accessible to only those employees whose job function require them to handle such documents.
- H. When outside a secure area, take appropriate action to safeguard CJI:
 - 1. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
 - 2. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock and/or privacy screens.
- I. Lock or log off computer when not in immediate vicinity of work area to protect CJI.
- J. Employees shall not email or transmit by other means CJI such as LEADS or NCIC information unless using an encrypted transmission method.
- K. CJI may only be disseminated to another agency if the other agency is an authorized recipient of such information.

41.12.2 MEDIA SANITIZATION AND/OR DISPOSAL

- A. All electronic media containing CJI shall be sanitized, that is, overwritten at least three times or degaussed prior to disposal or released for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.).
- B. Electronic media that is required to be sanitized shall be brought to the city's ITS department to ensure the sanitation is completed according to proper standards.
- C. Physical media that is ready to be disposed shall be shredded.

41.12.3 BREACH NOTIFICATION AND INCIDENT REPORTING

- A. Employees shall promptly report any potential data breaches, loss of CJI or other suspicious data system activity to city's ITS or a public safety systems specialist.
- B. The ITS department utilizes various software and hardware monitoring systems that report suspicious activity and potential unauthorized access attempts. All public safety systems specialists shall monitor various logs and system notifications that may be indicative of unauthorized system access.
- C. Public safety systems specialists and ITS personnel shall immediately begin mitigation procedures to limit damage and continued unauthorized access.
- D. Any data breach or loss that may affect CJI shall be reported by a public safety systems specialist to the appropriate criminal justice information authority personnel.