# CHAMPAIGN POLICE DEPARTMENT

POLICY and PROCEDURE | POLICY NUMBER: 82.5

SUBJECT: PHYSICAL PROTECTION OF CRIMINAL JUSTICE INFORMATION | EFFECTIVE DATE: 04/15/15 | REVISED DATE:

REFERENCE ILEAP:

INDEX AS:

82.5.1 PHYSICALLY SECURE LOCATION
82.5.2 VISITOR ACCESS
82.5.3 AUTHROIZED PHYSICAL ACCESS
82.5.4 ROLES AND RESPONSIBILITIES
82.5.5 PENALTIES

PURPOSE:

The purpose of this policy is to provide guidance for Department personnel, private vendors, and outside contractors for the physical, logical, and electronic protection of Criminal Justice Information (CJI).

All physical, logical, and electronic access to devices which store, process, or transmit encrypted Criminal Justice Information (CJI) must be properly authorized, controlled, and documented. This policy focuses on the access control methods necessary to protect the full lifecycle of Criminal Justice Information (CJI) from both inside and outside threats and was developed in compliance with the Federal Bureau of Investigation Criminal Justice Information Security Policy (5.1).

DEFINITIONS:

POLICY:

**82.5.1 PHYSICALLY SECURE LOCATION**

A. A physically secure location is a facility or an area, room, or group of rooms within a facility with both physical and personnel security controls sufficient to protect Criminal Justice Information (CJI) and associated information systems.

B. The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

C. Restricted access areas within the Department shall be identified by a sign at the entrance.

**82.5.2 VISITOR ACCESS**

A. A visitor is defined as an individual who is not an employee but visits the Department on an occasional basis and has no unescorted access to physically secure locations within the Champaign Police Department where Criminal Justice Information (CJI) and associated information systems are located.

B. Visitors shall check in before entering a physically secure location by signing the visitor access log. The visitor's log shall include the name of the visitor, visitor's agency, purpose of visit, date of visit, time of arrival and departure, and name and agency of person visited.

   1. Each visitor shall be issued and prominently display at all times a Department issued visitor badge.

C. Visitors, including contractors, vendors, and delivery personnel, shall be escorted at all times unless they have successfully passed a national fingerprint-based background check and established a Security Addendum.

D. Visitors shall not be permitted to view screen information.

   1. The Department has purchased and installed security screens to minimize the potential for access to screen information.

E. Visitors not having legitimate business within restricted areas of the building will remain in public areas of the building.

F. Requests by groups for tours of the facility may only be granted by a supervisor.

**82.5.3 AUTHORIZED PHYSICAL ACCESS**

A. Only authorized personnel will have access to physically secure locations.

B. The Champaign Police Department will maintain a current list of authorized personnel.

C. The Champaign Police Department has implemented access and monitoring controls to ensure that only authorized personnel have access to Criminal Justice Information (CJI) and display mediums.

D. Authorized personnel will take all necessary steps to prevent and protect physical, logical, and electronic breaches from occurring.

E. All authorized personnel with physical and logical access to Criminal Justice Information (CJI) must:

   1. Meet minimum personnel screening requirements prior to being granted access to Criminal Justice Information.

      a. To verify identification, a state of residency and national fingerprint-based records checks shall be conducted within 30 days of assignment for all personnel who have direct access to Criminal Justice Information (CJI) or direct responsibility for maintaining or configuring computer systems or networks with direct access to Criminal Justice Information (CJI).

b. Unless escorted at all times, support personnel, private contractors, and custodial personnel with access to physically secure locations or controlled areas shall also be subject to state of residency and national fingerprint-based records checks. If conducted, these records checks shall be completed prior to granting access.

2. Complete security awareness training.

   a. Security awareness training shall be completed within six (6) months of access and every two (2) years thereafter.

3. Remain aware of others who are or may be present in secure areas before accessing confidential data or information and take appropriate steps to protect all confidential data or information.

4. Properly protect and not share any individually issued keys or computer passwords.

   a. Lost or compromised keys or passwords shall be reported immediately so that appropriate de-activation measures can be taken.

5. Properly protect Criminal Justice Information (CJI) from viruses, worms, Trojan horses, and other malicious code.

6. Appropriately monitor their internet and website usage.

7. Refrain from using personally owned devices to access Criminal Justice Information (CJI).

8. Take appropriate measures to protect electronic media and printed Criminal Justice Information (CJI) records when physically removed from secure areas.

9. Encrypt emails when electronic mail is used to transmit Criminal Justice Information (CJI).

10. Promptly report compromises in physical security or loss of Criminal Justice Information (CJI), laptop, thumb drive, etc.

11. Release Criminal Justice Information (CJI) only to properly vetted personnel.

12. Properly dispose of Criminal Justice Information (CJI) when no longer needed.

**82.5.4 ROLES AND RESPONSIBILITIES**

A. Terminal Agency Coordinator (TAC).

1. The Terminal Agency Coordinator (TAC) serves as the point of contact at the Champaign Police Department for matters relating to access to Criminal Justice Information (CJI). The Terminal Agency Coordinator administers Criminal Justice Information Systems programs within the agency and oversees the agency's compliance with FBI and State Criminal Justice Information Systems policies.

B. Local Agency Security Officer (LASO).

1. The Local Agency Security Officer shall:

   a. Identify who is using state approved hardware, software, and firmware and ensure that no unauthorized individuals or processes are allowed access to same.

   b. Identify and document how the equipment is connected to the state system.

   c. Ensure that personnel security screening procedures are being followed as stated in this policy.

   d. Ensure that the approved security measures are in place and working as expected.

   e. Support policy compliance and ensure that the CJIS System Agency Information Security Officer (CSA ISO) is promptly informed of any security incident.

C. Agency Coordinator (AC).

1. An Agency Coordinator (AC) is a staff member of the Contracting Government Agency (CGA) who manages the agreement between private contractors and the Champaign Police Department. When the Champaign Police Department contracts with a private contractor, the Agency Coordinator (AC) shall be responsible for the supervision and integrity of the system, the training and continuing education of private contractor employees, the scheduling of initial training and testing, certification testing, and all reports required by the National Crime Information Center (NCIC).

D. CJIS System Agency Information Security Officer (CSA ISO).

1. The CJIS System Agency Information Security Officer (CSA ISO) shall:

   a. Serve as the security point of contact to the FBI CJIS Division ISO.

   b. Document technical compliance with the CJIS Security Policy with the goal of ensuring the confidentiality, integrity, and availability of criminal justice information to authorized personnel.

   c. Document and provide assistance in implementing security-related controls.

   d. Establish procedures sufficient to discover, investigate, document, and report incidents which may endanger the security or integrity of Criminal Justice Information (CJI).

   e. Ensure that the Local Agency Security Officer (LASO) institutes appropriate incident

response and reporting procedures at the local level.

E. Information Technology (IT) Support.

1. In coordination with each of the above described roles, all vetted IT support staff will protect Criminal Justice Information (CJI) from compromise by performing the following:

a. Know where Criminal Justice Information (CJI) is stored, printed, and copied, and protect information subject to confidentiality concerns (whether in systems, archived, or on back-up media) until destroyed.

b. Be knowledgeable of Champaign Police Department technical requirements and policies, and take appropriate preventive measures and corrective actions to protect Criminal Justice Information (CJI).

c. Take appropriate actions to ensure maximum uptime of Criminal Justice Information (CJI) and expedited back-up restores by using agency approved practices for power back-up.

d. Protect the Champaign Police Department's Criminal Justice Information Systems from viruses, worms, Trojan horses, and other malicious code by installing and maintaining antivirus programs and scanning outside CDs, DVDs, and thumb drives prior to use.

e. Perform data back-ups and take appropriate measures to protect all stored Criminal Justice Information (CJI).

f. Ensure that only authorized and vetted personnel transport or have access to off-site back-ups or other media storage.

g. Ensure that all media released by the agency is properly sanitized or destroyed.

h. Identify applications, services, and information systems containing software or components by recently announced software flaws and potential vulnerabilities resulting from those flaws.

i. Implement access control measures and enable event logging for successful and unsuccessful: log-on attempts; password changes; attempts to access, create, write, delete, or change permissions; attempts to access, modify, or destroy audit log files.

j. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit Criminal Justice Information (CJI).

k. Manage and monitor all user accounts in coordination with the Terminal Agency Coordinator (TAC) and restrict passwords as required.

l. Take appropriate actions to protect Criminal Justice Information (CJI) and related data from unauthorized public access.

m. Control access and monitor, enable, and update configurations of boundary protection firewalls.

n. Enable and update personal firewall on mobile devices.

o. Ensure that confidential data is only transmitted on secure network channels using encryption and advanced authentication.

p. Ensure that any media which is removed from a physically secure location is encrypted in transit.

q. Refrain from using default accounts on network equipment that passes Criminal Justice Information (CJI).

r. Ensure that law enforcement networks with Criminal Justice Information (CJI) are on their own network and accessible only by authorized personnel who have been vetted by the Champaign Police Department.

s. Keep the Champaign Police Department informed as to all scheduled and unscheduled maintenance and./or downtimes.

F. Front Desk and Visitor Sponsoring Personnel.

1. The administration of visitor check-in / check-out procedures is the responsibility of Front Desk staff.

**82.5.5 PENALTIES**

A. A violation of any term of this policy may result in:

1. Loss of access privileges;

2. Discipline, up to and including termination;

3. Criminal prosecution; and

4. Civil liability.

ISSUING AUTHORITY

Anthony D. Cobb
Chief of Police
Champaign Police Department