Personnel Security Policy Sample

(Sample written policy to assist with compliance)

1.0 Purpose

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the purpose of gaining access to the physical, logical, and electronic LEIN-based Criminal Justice Information (CJI).

2.0 Policy

2.1 Identity Verification

To verify identification, the Terminal Agency Coordinator (TAC) will ensure a MI and FBI fingerprint based record check has been conducted, within 30 days of assignment of all personnel with direct access to LEIN-based CJI and all personnel with direct responsibility to configure and maintain systems, networks, and databases with direct access to CJI.

2.2 Name Based Records Check

The TAC will conduct a name based records check CHRI using, Purpose Code J, for all personnel stipulated in section 2.1.

3.0 Qualifiers

All requests for access shall be made as specified by the MSP CSO.

- If a felony conviction of any kind exists, *[agency name]* shall deny access to LEIN-based CJI.
- *[Agency name]* may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed may support a possible exception by the CSO.
- If a record of any other kind exists, *[agency name]* shall not grant LEIN- based CJI access until the CSO has reviewed the record to determine of CJI access is appropriate.
- If the person appears to be a fugitive or has an arrest history without conviction, the CSO will review the record to determine if CJI access is appropriate.
- If the person is employed by a Non-Criminal Justice Agency (NCJA), the CSO, and *[agency name]* maintaining management control, shall review the record to determine if LEIN-based CJI access is appropriate.
- If a *[agency name]* employee, IT staff, etc., currently has access to LEIN-based CJI and is subsequently arrested and/or convicted, continued access to CJI shall be determined by the CSO.
- If the CSO determines that access to LEIN-based CJI by the person would not be in the public interest, access shall be denied and *[agency name]* shall receive written notice of the access denial.
- Support personnel, contractors, and custodial/maintenance workers with access to physically secure locations, or controlled areas during CJI processing, shall be subject to MI and FBI fingerprint-based record checks unless escorted by *[agency name]* authorized personnel at all times.
- As a best practice, individual CHRI background checks will be conducted by the *[agency name]* TAC every five years.

4.0 Contractor and Vendor Qualifiers

- Prior to granting access to LEIN-based CJI, *[agency name]* TAC shall verify identification with MI and FBI fingerprint-based record checks for retained contractors and vendors.
- The TAC will conduct a name based records check CHRI using, Purpose Code J, for all personnel stipulated in this section.

SAMPLE

- If a record of any kind is located, *[agency name]* shall delay system access pending review of the criminal history record information.
- When identification of the applicant with a criminal history has been established by fingerprint comparison *[agency name]* shall review the matter.
- A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified from LEIN-based CJI access.
- Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.

5.0 Access List of Personnel
[Agency name] TAC shall maintain a current list of personnel with authorization to access LEIN-based CJI and shall, upon request, provide a copy of the access list to the CSO.

6.0 Misdemeanor Offense(s)
Applicants with a record of misdemeanor offense(s) may be granted LEIN-based CJI access if the CSO determines the nature and severity (not punishable by more than one year) of the offense(s) do not warrant disqualification.

7.0 Reassigned/Transferred/Retired/Terminated/Resigned Personnel
[Agency name] TAC shall review LEIN-based CJI access authorizations when personnel are reassigned or transferred to other positions within *[agency name]* and initiate appropriate actions such as closing/establishing accounts and changing system access. The same is true for terminated/retired/resigned personnel. (*See User Account – Access Validation Policy).*

8.0 Penalties
Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and /or termination.

Other Related Resources:
- FBI CJIS Security Policy - Michigan Addendum
- User Account – Access Validation Policy (Required)

SAMPLE