LEADS MANUAL
Security Policy

SECURITY POLICY – Table of Contents

INTRODUCTION

This Policy is issued in addition to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy, which has been formed by presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council). The LEADS Security Policy is meant to be more inclusive than the CJIS policy and in no case will it be less restrictive.

User agencies must comply with the FBI CJIS Security Policy and all requirements specified in this document. Noncompliance with a requirement is sanctionable effective immediately except where a different deadline has been indicated. All new agency systems or upgrades connecting to the LEADS network must be in full compliance prior to being approved for connection.

The sanction process as defined in the LEADS Administrative Rules will be used for technical security violations. Exceptions to the progressive sanction process may be authorized by the CJIS Security Officer (CSO), if in his/her opinion, circumstances warrant such action.

This Policy may be disseminated to LEADS user agency personnel and vendors who have entered into contracts with LEADS user agencies.

PURPOSE

The FBI CJIS Security Policy and this Policy provide Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to the LEADS and FBI CJIS Division systems. This minimum standard of security requirements ensures continuity of information protection. The essential premise of the LEADS and FBI CJIS policies is to provide the appropriate controls to protect criminal justice information (CJI), from creation through dissemination; whether at rest or in transit.

CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

Criminal history record information (CHRI) and CJI obtained through LEADS routinely becomes a part of investigative case files provided to the county prosecutor for state criminal proceedings. When a prosecutor determines CHRI/CJI should be given to defense counsel in response to a valid demand for discovery under Ohio Criminal Rule 16, a prosecutor may turn the information over to defendant's counsel. The defendant may only have access to the defendant's own CHRI/CJI.

All other CHRI/CJI obtained through LEADS shall be marked, in accordance with Ohio Criminal Rule 16(C), with "Counsel Only." In addition, defense counsel shall be advised in writing that "The criminal justice information obtained through the Law Enforcement Automated Data System is protected by federal and state law including, but not limited to, 28 CFR Part 20, 2913.04(B) of the Ohio Revised Code, and Chapter 4501:2-10 of the Ohio Administrative Code. Dissemination of LEADS information, other than the defendant's own CHRI/CJI to the defendant, is considered a misuse of information obtained through the Law Enforcement Automated Data System and will be prosecuted accordingly. Also, dissemination beyond defense counsel or defense counsel's agents or employees may constitute a violation of Ohio Criminal Rule 16(C) and subject counsel to further disciplinary action."

Proper Access, Use, and Dissemination of Non-Restricted Files Information

Access, use, and dissemination of the LEADS activity report is restricted to criminal justice agencies for the purposes of the administration of criminal justice. The LEADS activity report, excluding CHRI and CJI, may be provided to an arbitrator and/or bargaining unit representative, as necessary, for use in collective bargaining proceedings. Any further transmission or dissemination of the LEADS activity report is governed by CSO authority in other circumstances.

Ohio Bureau of Motor Vehicles Records

The Ohio Bureau of Motor Vehicles (BMV) requires all driver and vehicle registration records, which include but are not limited to, the records of all Ohio and out-of-state drivers who have been convicted of a traffic offense in the State of Ohio to be accessed and disclosed only for the administration of criminal justice. Further, the Ohio BMV requires agencies to access, use, and secure these records in compliance with Ohio Revised Code sections 149.43, 4501.15, 4501.27 (commonly known as the Driver Privacy Protection Act), 4507.53, 1347.15; and Ohio Administrative Code 4501:1-12-02; and 18 U.S.C. 2721-2725. Any security breach involving Ohio BMV records shall immediately be reported to LEADS.

POLICY AND IMPLEMENTATION

Security Incident Response

LEADS Agencies shall immediately report security-related incidents that impact criminal justice agency systems or have the potential to impact LEADS systems or data to the LEADS Control Center at 1-800-589-2077.

Examples of such incidents include - but are not limited to - denial of service attacks, network intrusions, session hijacking, theft of mobile data terminals, viruses, malware, worms, etc. The LEADS Control Center will immediately contact the LEADS ISO.

If an agency's system or network is compromised to the point that a direct threat exists to the security of LEADS, the LEADS Security staff will direct the agency to disconnect their

equipment from the network. Defensive measures will be implemented by LEADS to limit exposure to further threats from the agency until the situation is contained and remedied.

The IT Security Incident Response Form shall be completed as soon as possible, but no more than seven days after the incident occurred.

Misuse of LEADS data, such as improper dissemination, should be reported directly to LEADS Administration at 1-800-589-2077.

Configuration Management

Access Restrictions for Changes

Any changes to software or hardware that transport, store or process CJI shall have LEADS approval prior to implementation and or upon request. An updated diagram shall be provided to LEADS prior to implementing new or changing existing systems that transport, store or process CJI. Refer to CJIS Security Policy Section 5.7.1.2 for network diagram requirements.