

MANUAL OF ADMINISTRATIVE AND OPERATIONAL GUIDELINES

Requirements for Agency Compliance

Approved and Adopted – July 7, 2011



TABLE OF CONTENTS

ARTICLE I	INTRODUCTION	ERROR! BOOKMARK NOT DEFINED.
SECTION 1	PURPOSE.....	1
SECTION 2	LEAP OVERVIEW	1
SECTION 3	LEAP ADVISORY COMMITTEE AND THE NORTH CENTRAL TEXAS COG	2
SECTION 4	PROJECT DESCRIPTION.....	3
SECTION 5	USE OF DATA AND PROBABLE CAUSE	4
SECTION 6	RESPONSIBILITY FOR RECORDS.....	5
SECTION 7	POLICY	6
SECTION 8	SECURITY	7
SECTION 9	PROJECT DISCIPLINE.....	8
ARTICLE II	LAWS	10
ARTICLE III	STANDARDS	11
SECTION 1	STANDARDS FOR INQUIRY RESPONSE.....	11
SECTION 2	STANDARDS FOR RECORD ENTRY AND UPDATES	12
SECTION 3	STANDARDS FOR AVAILABILITY	13
SECTION 4	STANDARDS FOR EQUIPMENT AND TECHNOLOGY COMPATIBILITY.....	13
SECTION 5	STANDARDS FOR SERVICES AVAILABILITY.....	13
ARTICLE IV	PARTICIPATING AGENCY RESPONSIBILITIES	14
SECTION 1	MANDATORY REQUIREMENTS	14
SECTION 2	OPTIONAL REQUIREMENTS.....	14
ARTICLE V	LEAP ADVISORY COMMITTEE	16
SECTION 1	ADVISORY COMMITTEE.....	16
SECTION 2	LEAP ADVISORY COMMITTEE ACTIVITIES	16
SECTION 3	ADVISORY COMMITTEE MEMBERSHIP.....	18
SECTION 4	CJIS SECURITY SUB-COMMITTEE	18
ARTICLE VI	LEAP SECURITY	19
SECTION 1	LEAP SECURITY GATEKEEPER.....	19
SECTION 2	INFORMATION SECURITY	19
SECTION 3	COMPUTER SECURITY	20
SECTION 4	PERSONNEL SECURITY.....	21
ARTICLE VII	LEAP ACCESS RULES	22
SECTION 1	LEVELS OF ACCESS TO LEAP	22
SECTION 2	USER ACCESS	22
SECTION 3	ADMINISTRATIVE ACCESS	24
SECTION 4	SECURITY ACCESS	24
SECTION 5	INFORMATION ENTRY	25
SECTION 6	INFORMATION MODIFICATION.....	26
SECTION 7	INFORMATION PURGES / CANCELLATION	26
SECTION 8	ALERTS.....	26
SECTION 9	ERROR MESSAGES	27
SECTION 10	ADMINISTRATIVE MESSAGES	27
ARTICLE VIII	QUALITY CONTROL.....	28
SECTION 1	MAINTAINING NETWORK INTEGRITY	28
SECTION 2	MAINTAINING THE INTEGRITY OF LEAP RECORDS	30
SECTION 3	QUALITY CONTROL.....	31
SECTION 4	VALIDATION	32
SECTION 5	RETENTION OF LEAP SEARCH RESULTS	32

SECTION 6	FILE REORGANIZATION AND PURGE SCHEDULE	33
ARTICLE IX	CJIS SECURITY SUB-COMMITTEE.....	34
SECTION 1	THE CJIS SECURITY SUB-COMMITTEE.....	34
SECTION 2	LEAP CJIS SECURITY PROCEDURES.....	36
SECTION 3	INTRODUCTION TO LEAP SANCTIONS	42
SECTION 4	SANCTIONS	43
SECTION 5	REINSTATEMENT.....	44
ARTICLE X	DEFINITIONS.....	46
ARTICLE XI	LEAP USER AGREEMENT	48
ARTICLE XII	MISCELLANEOUS PROVISIONS.....	52
ARTICLE XIII	ACKNOWLEDGEMENT	53

ARTICLE I

SECTION 1 PURPOSE

The purpose of this Manual of Administrative and Operational Guidelines (MAOG) is to document administrative procedures, operational guidelines and responsibilities of participating agencies and users with respect to LEAP operation, usage and maintenance. This document is intended to be a “living document” which will be updated periodically by the LEAP Advisory Committee and from the lessons learned from any security events as well as security program audits.

SECTION 2 LEAP OVERVIEW

LEAP is a multi-jurisdictional integrated justice data sharing and data analysis service under the governance of the LEAP Advisory Committee with sponsorship by the North Central Texas Council of Governments (NCTCOG). LEAP collects data from a variety of automated commercial, local, state and federal law enforcement and justice information systems on a frequent basis; reorganizes the data for easy access and analysis; and distributes the data and accompanying analysis to authorized users, also known as subscribers.

In an environment where violent crime is increasing at a rate more than 50% greater than the growth of the US population, city and county governments must seek ways to combat this disconcerting trend. Traditional solutions call for increased staffing to enhance the law enforcement officer/citizen ratio. Yet, violent crime is even increasing in municipalities with the highest officer/citizen ratios. Adding staff may be necessary but it is no longer sufficient as a solution to thwart the increases in violent crime.

Technology, however, can offer municipalities an edge in this escalating war on crime by providing “force multipliers” that expand the effectiveness and efficiency of existing staff – regardless of the officer/citizen ratio.

As additions to law enforcement staff alone fail to reduce the accelerating trends in violent crime, municipalities must employ additional complementary and strategic approaches that give their public safety initiatives greater leverage against the criminal element.

Better and more rapid availability of information can provide such leverage.

And since geopolitical boundaries do not inhibit the activities of criminals, a multi-jurisdictional shared data and shared analysis system that spans the artificial geographic boundaries of city or county lines can provide valuable information necessary to locate suspects or criminals who may live outside of a municipality but conduct their often violent trade within city or county limits.

Once an operational shared data and analysis system infrastructure is in place, other information technologies, such as license plate recognition, bait car placement/monitoring and video surveillance can be more easily implemented and the success of those programs managed through the automatic metrics available in the shared data and analysis system.

SECTION 3 LEAP ADVISORY COMMITTEE AND THE NORTH CENTRAL TEXAS COUNCIL OF GOVERNMENTS

The North Central Texas Council of Governments was established in January 1966, authorized by the State of Texas enabling legislation (Chapter 391 – Local Government Code), to assist local governments in planning for common needs, cooperating for mutual benefit, and coordinating for sound regional development. The immediate North Central Texas Council of Government region is a sixteen-county metropolitan area centered on the Dallas and Fort Worth Metroplex. It has a growing population, currently over 6.5 million, which is larger than thirty seven states, and an area of 12,800 square miles, which is larger than nine states. NCTCOG currently has 231 member governments. The membership includes 16 counties, 164 municipalities, 23 independent school districts, and 28 special purpose districts.

The purpose of NCTCOG is to strengthen both the individual and collective power of local governments -- and to help them recognize regional opportunities, resolve regional problems, eliminate unnecessary duplication, and make joint regional decisions -- as well as to develop the means to assist in the implementation of those decisions.

While focused on its immediate constituency of government agencies within the 16 county Dallas – Fort Worth Texas Metroplex region, NCTCOG recognizes the economies of scale in shared resource information technology that enhance the economic benefit for each supported law enforcement and justice agency. Accordingly NCTCOG has encouraged the scope of LEAP to include all local law enforcement and justice organizations throughout the United States with respect to information sharing.

In order to execute on its shared information technology resource vision, NCTCOG entered into a public private partnership with private sector organizations, which, through collaboration with NCTCOG, created the Law Enforcement Analysis Portal (LEAP) to address the needs of public safety and justice professionals. NCTCOG initiated and sponsors the full governance of LEAP to local law enforcement in the creation of the LEAP Advisory Committee.

The LEAP ADVISORY COMMITTEE is the governance over information sharing of data owned by the law enforcement agencies sharing their data with LEAP. Composed only of law enforcement professionals, the Advisory Committee determines the policy decisions associated with LEAP and provide the direct guidance of LEAP as the representative body for law enforcement agencies.

SECTION 4 PROJECT DESCRIPTION

LEAP is a multi-state analysis and data sharing system for sworn officers and civilians in certified law enforcement agencies including independent school district police forces, police departments and sheriff offices in those states in which LEAP operates. LEAP currently operates in the state of Texas and plans to expand into contingent states, federal partnerships and Native American tribes as they come into the organization. The LEAP program is an information sharing tool for agencies which currently have electronic Records Management System (RMS) and other law enforcement information system capabilities. These collaborations are focused on the following specific public safety needs:

- 1. To support electronic information sharing (data interoperability) and algorithmic tool based analysis of this data across jurisdictional lines;**

2. To offer attractively affordable data center hosted software solutions such as Records Management System and other law enforcement information systems to local law enforcement and justice agencies;
3. To sustain the use of these utilities and tools with training, continuing education and long distance learning in collaboration with public safety academies and institutes of higher education; and
4. To include other public safety agencies at the local, state and federal levels that serve and protect their citizens from threats of crime, violence and terrorism.

SECTION 5 USE OF DATA AND PROBABLE CAUSE

The data content of the LEAP program will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures or any activity that would directly result in providing sworn testimony in any court. Information available in the LEAP program is not probable cause, but indicates that data, a report or other information exists in the Records Management System or other law enforcement or judicial information system of an identified participating agency. An information element in the LEAP program should be considered only one component in effective law enforcement for building an investigative case that could lead to probable cause for arrests, searches and seizures, court testimony, etc.

The data from the LEAP program is not considered, and should not be used for, original documentation for probable cause by any participating agency.

Correct LEAP program procedures, as agreed upon by the Advisory Committee, requires the agency which provided access to the data be contacted by the inquiring user to confirm that the data is accurate and up-to-date. In some circumstances, the data element which must be confirmed with the originating agency may be the major or only element necessary to “initiate” an investigation, obtain a search warrant, detain a subject or make an arrest. An example might be a confirmation of law enforcement information existing in a participating agency’s RMS on an individual or description of a vehicle or property. The inquirer must have a confirmation made from the original agency and not utilize the documentation obtained from the LEAP program to support the initiation of investigations, searches, or other activity that would likely lead to testimony. The confirmation of validity from the originating RMS, regardless of how long it had been in the LEAP program, may be enough cause to take appropriate and reasonable action.

SECTION 6 RESPONSIBILITY FOR RECORDS

- 1. The LEAP program which consists of information from existing law enforcement and justice information systems and records must be kept accurate and up-to-date. Agencies and courts that contribute records to the LEAP program maintain total control and ownership of those records and are responsible for their accuracy, timeliness, and completeness.**
- 2. Stringent administrative procedures and controls to ensure that accurate data is entered in computerized criminal justice information systems are important. Combining stringent administrative controls with proper evaluation by the individual receiving the query response can prevent lost court cases, civil liability suits, false arrests, and civil or criminal charges against the law enforcement agency employee. The LEAP Advisory Committee, the owners of the LEAP program, will maintain the integrity of the collected data through:**
 - a. Engaging a third party security organization to insure the technical integrity of the LEAP program;**
 - b. Contracting with an expert operator for the LEAP program for monitoring and maintaining data edits and updates from the participating records management systems; and**
 - c. Demanding regular scheduled updates, not to be more than 24 hours delayed, of the data contributed by participating agencies to insure that current and accurate up to date information is being maintained within the LEAP program.**
- 3. All participating agencies in the LEAP program will be responsible to insure integrity of the data through:**
 - a. Insuring the identification and elimination of common types of errors in their law enforcement data contributed to the LEAP program;**
 - b. Purging of their records maintained for a period of time, as prescribed by laws, ordinances, policies and procedures; and**
 - c. Quality control checks.**
- 4. The LEAP program makes network accessible data and centralized law enforcement data immediately available to authorized participating agencies within a given region.**

The success of this project depends upon the extent to which patrol officers, investigators, analysts, agents, and other law enforcement employees intelligently use it in day-to-day operations.

5. This document intends to instruct and is designed to guide participants in using the LEAP program. No technical system can be expected to produce results unless it is properly used. The standards and procedures set forth should be strictly followed, as every exception tends to degrade the performance of the system and the integrity of the data stored in the LEAP program.
6. All inquiries regarding any specifics about the LEAP program should be addressed to the LEAP Advisory Committee.

SECTION 7 POLICY

The LEAP Advisory Committee establishes policy with respect to the philosophy, concept, operational principles and security policy of the LEAP program for the region. In its deliberations, the Advisory Committee places particular emphasis on the continued compatibility of the LEAP program; network security; and rules, regulations, and procedures to maintain the integrity of the LEAP program and the records shared over the system.

The LEAP governance and advisory process is composed of two major components, the LEAP Advisory Committee and its subcommittees. The LEAP Advisory Committee is responsible for reviewing policy issues and appropriate technical and operational issues related to the LEAP program and, thereafter, for making appropriate recommendations. The Advisory Committee is made up of Federal, State, County and Municipal agency heads or their principal designees, and is limited to those agencies who are actively participating in the LEAP program by contributing law enforcement data to the project, accessible by all parties. The Advisory Committee operates as a democratic body with an established charter, by-laws, and memorandum of understanding with the sponsorship of NCTCOG's Executive Board.

The LEAP program user group consists of administrative, operational and technical experts from the participating departments. It is the responsibility of the user groups to

recommend policy, procedures and changes for the LEAP program in order to enhance its operability and ensure access by all its participants.

SECTION 8 SECURITY

There is no federal level legal or policy prohibition against dissemination of information contained in the LEAP program for law-enforcement purposes, which consists of derivative law enforcement information only. If no state/county/municipal law, ordinance or policy prohibition exists towards the dissemination of information contained in the LEAP program, then authorized dissemination of those records may be conducted for law-enforcement purposes only, and is subject to the discretion and regulations of the participating agency to retain full control of that information.

Information may be withheld from the LEAP program at the discretion of each agency due to acceptable criminal justice priorities, case sensitivity, source sensitivity, budget or legal reasons, or reasons determined by the Advisory Committee to be legitimate.

An agency participating in LEAP must assume responsibility for and enforce security with regard to all users within that agency.

LEAP uses hardware and software controls to help ensure security. However, final responsibility for the maintenance of the security and confidentiality of law enforcement information within the LEAP program rests with the individual agencies participating in LEAP.

All federal, state, county and municipal agencies participating in the LEAP program are required to adhere to the security guidelines as set forth in some parts of the United States Department of Justice Regulations governing the dissemination of criminal records and criminal history information, as published in the Federal Register on May 20, 1975, and August 7, 1976 (Title 28, Code of Federal Regulations, Part 20).

Data contributed to the LEAP program consists of documented law enforcement information and must be protected to ensure correct, legal, and efficient dissemination and use. It is incumbent upon any agency utilizing or having access to the LEAP information

sharing system to implement the necessary procedures to make that access secure from any unauthorized use. Any departure from this responsibility warrants the removal of the offending agency from further access to the LEAP program as specified by the Advisory Committee directives.

Information can be obtained from the LEAP program both directly and indirectly. Direct access is through existing user authenticated access to the network from internet enabled devices or through the indirect dissemination of law enforcement information outside of the agency with specified access to the system. Indirect access or non-network access outside of an agency with direct access to the LEAP is not permitted without express written permission via executed Memorandum of Understanding between the originating agency for the law enforcement data and the LEAP Advisory Committee governing the dissemination of the data contained within the LEAP program to nonparticipating agencies. Such access will utilize a data selection and transmittal component known in the LEAP program as the “Data Spigot.”

Any agency allowing access to the LEAP program must insure that the person being granted access to the LEAP program has had appropriate background checks conducted by the agency allowing access and is authorized to receive the law enforcement data contained therein. Dissemination of law enforcement information to all authorized users is not discretionary and is governed by the regulations of the originating agency of that information and rules established by the Advisory Committee.

Unauthorized request, use, dissemination or receipt of LEAP information could result in administrative sanctions, civil or criminal proceedings being brought against the agencies and/or individuals involved.

SECTION 9 PROJECT DISCIPLINE

To help ensure the proper operation of the LEAP program, the standards, procedures, formats, and criteria mentioned in this document must be strictly followed. In this respect, the LEAP Advisory Committee must not only follow the rules set forth, but must also ensure that participating agencies are doing the same. In doing so, the Advisory

Committee will develop and adopt a set of security standards and policies for the project to be complied with by all participating agencies.

Complete, accurate, and timely records are essential to ensure the integrity of the LEAP program. All participating agencies are encouraged to contribute all levels of structured and free text law enforcement records in a timely manner to afford the maximum accessibility of law enforcement information to the law-enforcement community in an up-to-date fashion. Although use of the LEAP program is voluntary, delayed entries of records into the LEAP program reduces or eliminates the possibility of addressing criminal or potential terrorist activities or having a significant impact on organized criminal problems within the region.

Promptness in contributing, modifying, locating, or eliminating records in the system helps keep the LEAP program free of outdated information.

The LEAP program also provides information for decision making by first responders, investigators, analysts, and the executive management of the participating law-enforcement agencies. The information furnished through the LEAP program must be evaluated along with other facts known to officers, investigators, analysts, and administrators prior to action being initiated.

ARTICLE II LAWS

This Manual of Administrative and Operational Guidelines for LEAP, incorporates the following laws and standards, all of which are recorded hereinafter as addendums:

- 1. Code of Federal Regulations (CFR), Title 28--Judicial Administration, Chapter I-- Department Of Justice, Part 20--Criminal Justice Information Systems (CJIS)**
- 2. CJIS Security Policy, Version 4.2, September 2005, Approved by the CJIS Policy Board, June 2005**
- 3. US Department of Justice (DOJ) Federal Bureau Of Investigation (FBI) Criminal Justice Information Services Security Addendum**
- 4. National Crime Information Center (NCIC) 2000 – Standards and Sanctions**
- 5. Texas Government Code § 411.083. Dissemination Of Criminal History Record Information**
- 6. US Department of Homeland Security (DHS) Homeland Security Advisory Council, Private Sector Information Sharing Task Force on Homeland Security Information Sharing Between Government and the Private Sector, August 10, 2005**
- 7. Homeland Security Lessons Learned Information Sharing (LLIS) Intelligence and Information Sharing Initiative Homeland Security Intelligence Requirements Process**
- 8. US DOJ National Criminal Intelligence Sharing Plan, October 2003**
- 9. US DOJ / DHS Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal and Federal Level, Law enforcement Intelligence Component, Level I, July 2005**
- 10. US DOJ FBI CJIS Division, Law Enforcement National Data Exchange, Concept of Operations, Version 1.5, May 1, 2006**

ARTICLE III STANDARDS

The following standards have been developed for the LEAP program and document the metrics by which LEAP behavior and performance is measured. Such metrics are only recommended until the LEAP user base reaches a sustaining user volume, at which time the metrics will become mandatory and will constitute the required service level.

The use of “effective information sharing” to help the criminal justice community perform its duties not only means providing access to and obtaining detailed information from pertinent computerized databases and RMS’s, but also includes the amount of time required to access the data. While an inquiry, or update message may contain specific and detailed information, the analysis message (communication) could be very ineffective if it cannot be transmitted to the querying party and a response cannot be received from the system within a reasonable amount of time. The rapid transmission of all messages is extremely important, and standards have been developed to ensure that messages are transmitted and processed within a reasonable amount of time.

To ensure the integrity of the system, certain policies and standards must be created, adopted, and followed. Through these policies and standards, a tool of measurement is provided against which the LEAP program can measure the performance of the component parts of the LEAP program as a whole. These policies and standards also must address the specific areas of compliance of the “special” case situations.

SECTION 1 STANDARDS FOR INQUIRY RESPONSE

Based on high speed internet broadband access of average bandwidth not less than 1 Mbps for the attached inquiry device:

1. The recommended average message response time for a single screen inquiry from the remote agency access device to the LEAP program server and back to the remote agency access device should not exceed 15 seconds. Note that the system will request tighter inquiry parameters if more than 10,000 items are returned from the query.
2. The recommended average message response time for a multiple compound screen inquiry from the remote agency access device to the LEAP program server and back to the remote agency access device should not exceed 30 seconds. Note that the system will

request tighter inquiry parameters if more than 10,000 items are returned from the query.

3. The recommended average analytical response time from an agency interfaced with the LEAP program server should not exceed 45 seconds after transmission of the inquiry, with 15 of the 45 seconds allocated to the transmission to, processing by, and return of the response from the LEAP program server as described in Standards 1 and 2 above.
4. An additional 15-second allowance can be made for additional system interfaces. These interfaces will include servers to local area or wide area networks, intranets, and wireless communication systems (commercial and private). For example, mobile units connected to a wireless communications system and then connected to a metropolitan server that is interfaced with, and then connected to the LEAP program will be allowed a 60-second total response time from the initial inquiry.

Note: Average time should be based upon a compilation over a 30-day period. Abnormal operating times, such as during the installation of a new computer, should be excluded from the 1-month compilation.

SECTION 2 STANDARDS FOR RECORD ENTRY AND UPDATES

Any law enforcement agency having investigative authority, jurisdiction within the respective region, having agreed to fully participate in the LEAP program and having agreed to the principles of the MOU, will as soon as reasonable or possible, ensure investigative data is contributed to the LEAP program.

1. The Advisory Committee shall be responsible for assuring that every agency that has access and has agreed to the conditions of the data sharing MOU vetted between the agency and the Advisory Committee will contribute investigative records to the LEAP program.
2. Every agency that contributes records to the LEAP program must assure that information confirmation is available for all records, within a 24 hour period (or next business day) from the time of inquiry.
3. Every participating agency is responsible for the removal from the LEAP program of any investigative record as soon as that agency is aware that the record is no longer valid by removing or deleting the record from its RMS or other law enforcement information system from which LEAP data is collected, resulting in the removal of the

record automatically from LEAP. It is the responsibility of the LEAP program to process the update to the LEAP program.

SECTION 3 STANDARDS FOR AVAILABILITY

The LEAP program availability goals shall be 100 percent with 99 percent as minimum acceptable performance.

SECTION 4 STANDARDS FOR EQUIPMENT AND TECHNOLOGY COMPATIBILITY

Equipment and/or technological incompatibility shall not be sufficient justification for any agency to operate outside of the normal and approved LEAP program configuration.

SECTION 5 STANDARDS FOR SERVICES AVAILABILITY

Those services provided by the LEAP program to the participating agencies shall be provided to their approved users as prescribed by the Advisory Committee with the exception of:

1. Services specifically limited to System Administrators;
2. Services specifically limited to Security Administrators;
3. Services which are restricted to certain users by nature of federal, state, county or municipal laws, ordinances, policies and regulations governing access to certain types of investigative data;
4. Services that may be contrary to a state law or executive order.

“Users” include individuals employed by those law enforcement agencies approved by the LEAP Advisory Committee to execute a MOU and by Law Enforcement Executive acknowledgement and agreement with this Manual of Administrative and Operational Guidelines. Included are data contributors to the LEAP program and those individuals accessing data from the LEAP program through any regional dispatch center, regional network, specific agency connection, electronic switch, wireless capability, or other approved computer interface.

The use of any LEAP services by any approved agency shall be in accordance with the instructions and procedures established by the MOU, this document, Security Policy and/or any regulations established by the Advisory Committee.

ARTICLE IV PARTICIPATING AGENCY RESPONSIBILITIES

SECTION 1 MANDATORY REQUIREMENTS

- 1. Participating agencies will enter into an appropriate Memorandum of Understanding with the Advisory Committee if the agency desires to contribute data to LEAP;**
- 2. Participating agencies will acknowledge and agree to be bound by the terms and conditions of this Manual of Administrative and Operational Guidelines for their “users” to access the LEAP program;**
- 3. Users will execute and agree to a LEAP User Agreement;**
- 4. Participating agencies will comply with and mandate compliance of all individual users enabled for LEAP access with each specific provision of these policies and procedures;**
- 5. Participating agencies will accept the responsibilities delegated to it by the Advisory Committee;**
- 6. Participating agencies will only assign LEAP subscriptions to agency/departmental users with agency or departmental email accounts; and**
- 7. Participating agencies may not use data, which was obtained by the agency from a LEAP query, to populate Intelligence or other searchable database.**

SECTION 2 OPTIONAL REQUIREMENTS

- 1. Participating agencies may, but need not, be a member of another statewide or nationwide intelligence system;**
- 2. Participating agencies may participate either voluntarily or under mandatory provision.**

A Participating Agency that collects LEAP data will collect and maintain the information and documentation supporting each LEAP record in compliance with existing criminal justice guidelines and its own Memorandum of Understanding with the Advisory Committee.

Participating Agencies will be subject to annual or otherwise scheduled audits to ensure that their access to LEAP is in compliance with these and other appropriate guidelines. In

most instances, Participating Agencies Internal Affairs or Professional Responsibility entity will be the conduit in conjunction with the LEAP Security Gatekeeper.

The Participating Agency's facility will be subject to unannounced security inspections (compliance audits) of LEAP usage performed by the LEAP Security Gatekeeper.

It is the responsibility of each participating agency to notify the LEAP Security Gatekeeper, and the Advisory Committee of any changes to the employment status of personnel within their respective agency whose access to LEAP might need to change.

ARTICLE V LEAP ADVISORY COMMITTEE

SECTION 1 ADVISORY COMMITTEE

The LEAP Advisory Committee shall be appointed by the NCTCOG's Executive Board for the Advisory Committee to insure that data collected from local law enforcement and justice agencies are appropriately secured and maintained.

The Committee shall strive to achieve the following objectives:

- 1. Represent law enforcement agencies who contribute data to the LEAP program by providing oversight on security implemented in LEAP and to protect contributed data from distribution outside the LEAP program.**
- 2. Provide suggestions and recommendations regarding how the LEAP program can better enhance public safety and professional law enforcement throughout the states in which LEAP operates.**
- 3. Represent local law enforcement and develop a direct communications channel and cooperative relationship on behalf of the LEAP program with:**
 - a. The Departments of Public Safety and other criminal justice officials in the states in which LEAP operates;**
 - b. Federal law enforcement agencies and High Intensity Drug Trafficking Areas;**
 - c. Local, state and national law enforcement task forces and programs in the states in which LEAP operates that might benefit from data and analysis sharing programs;**
 - d. Government and private sector entities in the states in which LEAP operates that might benefit from data and analysis sharing provided by LEAP.**

SECTION 2 LEAP ADVISORY COMMITTEE ACTIVITIES

The following activities will be advanced and promoted by the LEAP Advisory Committee:

- 1. Develop a regional interstate crime strategy that incorporates all levels of law enforcement within the community in the acquisition of information, as well as the identification of the significant criminal and terrorism concerns where the LEAP effort will have a significant impact. This strategy will identify and outline regional crime concerns, operational strategies to overcome these concerns, information needs to**

support the operational strategy, and measurable parameters from which to gauge success.

2. **Provide the mechanism to determine the appropriate use of the LEAP service and the consequences for agencies and individuals that fail to comply with such appropriate use including the withholding of services to those participating agencies and/or individuals deemed to have failed to comply after a specified formal review and recommendation of sanctions by the Committee.**
3. **Develop legal and regulatory compliance for the LEAP effort. This includes appropriate guidance and oversight to comply with all laws and regulations regarding citizen rights, confidentiality, and to insure that privacy is upheld and protected. Towards this end, the Committee will identify procedural measures to address compliance with all legal and regulatory requirements associated with retention, use, dissemination, and purging of information collected in support of the LEAP effort.**
4. **Approve the creation and resulting terms and conditions of data sharing Memorandums of Understanding between participating law enforcement agencies for participation in the LEAP program, and to manage the compliance of participating agencies and subscribing individuals to all terms and conditions for the use of LEAP, as defined by the Manual of Administrative and Operational Guidelines.**
5. **Oversee operations and maintenance of the LEAP effort to include supplying requirements for the addition and deletion of LEAP users by the participating agencies, supplying requirements for the monitoring of security mechanisms to detect malicious and or unusual activities, supplying requirements for backup and restoration of information in the LEAP program and aiding in the accomplishment of user training.**
6. **Identify and explore opportunities for future sources of additional funding. This may require the sharing of personnel resources to prepare application(s) for grants or other sources of funding.**
7. **Evaluate enhancements for improving the operational, analytical, and technical aspects of the LEAP effort. The LEAP Advisory Committee will help establish a LEAP User Group and put in place processes and procedures to collect and evaluate recommendations for enhancements to the LEAP program.**

There will be two standing Sub-Committees on the Advisory Committee: the Nominating Sub-Committee and the CJIS Security Sub-Committee.

SECTION 3 ADVISORY COMMITTEE MEMBERSHIP

Membership in the Advisory Committee is limited to law enforcement professionals and is defined in the LEAP Advisory Committee By Laws.

SECTION 4 CJIS SECURITY SUB-COMMITTEE

The LEAP Advisory Committee shall maintain a CJIS Security Sub-Committee (CSC) as defined in the LEAP Advisory Committee By Laws.

ARTICLE VI LEAP SECURITY

SECTION 1 LEAP SECURITY GATEKEEPER

The LEAP Advisory Committee has and will continue to engage a third party independent auditor, hereinafter referred to as the “Gatekeeper.” The LEAP Gatekeeper is engaged to provide security services to the LEAP Advisory Committee with respect to the LEAP program.

SECTION 2 INFORMATION SECURITY

Participating Agencies shall maintain a security program which complies with the following elements:

- 1. The security plan will have solid, industry proven precautions in place to protect the confidentiality, integrity, and availability of the agency’s internal e-mail accounts.**
- 2. The Participating Agency shall assign a Point of Contact accountable for the management of their security program and liaison with the LEAP Gatekeeper.**
- 3. The Participating Agency shall document its security program in a Security Plan, usually the same plan as required by FBI CJIS to access NLETS or NCIC.**
- 4. The Participating Agency shall provide for a Security Training Program for all agency personnel engaged in the operation, security or maintenance of the computers and browsers accessing LEAP.**
- 5. The Participating Agency shall establish a security violation response and reporting procedure to discover, investigate, document, and report on all security violations. All violations of the respective agency’s Security Program, as discovered by the participating agency, shall be reported to the Advisory Committee, or the Gatekeeper. Conversely, the Advisory Committee or the Gatekeeper shall immediately report any alleged violation to the designated official in charge of the Security Program of that respective agency.**
- 6. The Participating Agency’s security program will be subject to annual review by the Gatekeeper.**

Information contained in LEAP is the property of the respective agency that provided the information. Access to this information is granted to “authorized users” of participating agencies with the understanding that use of this information is restricted to criminal justice

investigations. Indirect access to this information to other agency personnel is authorized with the same understanding.

The participating Agency shall ensure that its inquiries of data contained in LEAP and any subsequent dissemination conform to applicable LEAP policies and regulations as set forth in the Memorandum of Understanding and this Manual of Administrative and Operational Guidelines.

SECTION 3 COMPUTER SECURITY

While the computers used by authorized users to access LEAP need not be dedicated for this purpose; they must be protected against malicious code (such as viruses, Trojans, worm infestations, and spy ware) and hacking attacks through appropriate virus protection software and physical or software firewalls.

Only persons authorized by their respective department shall be granted access to LEAP. Logins and passwords are provided under the authority of the LEAP Advisory Committee. Once the Participating Agency's LEAP administrator has assigned a LEAP subscription to authorized users within the agency, it must be afforded proper security to ensure against unauthorized access by persons not properly vetted for access. Logins and passwords are not to be shared with other agency personnel.

Indirect access to LEAP information is authorized when its use is intended for criminal justice administration. Persons with LEAP access may share information obtained from LEAP with other law enforcement personnel. (This latter point is known as granting indirect access.)

All data associated with LEAP records shall be cached, stored and or disposed of in an appropriate and effective manner to prevent access by unauthorized personnel.

The Participating Agency shall establish a procedure for sanitizing all fixed storage media (e.g., disks, drives) which they may have used to store any data from or derived solely from LEAP at the completion of the Agreement and / or before it is returned for maintenance, disposal, or reuse. Sanitation procedures include overwriting the media and or degaussing

the media. If media cannot be successfully sanitized, it must be returned to the LEAP Gatekeeper for appropriate destruction.

Terminals or access devices which have LEAP access must be protected by firewall-type devices that implement a minimum firewall profile to provide a point of defense.

Security violations can justify termination of the user's access to the LEAP program.

SECTION 4 PERSONNEL SECURITY

Appropriate background investigations must have been conducted on all agency employees being authorized for access to LEAP.

The Participating Agency's Security Officer (or agency LEAP Point of Contact) will ensure and acknowledge that each employee with access to LEAP reviews this Manual of Administrative and Operational Guidelines and accepts the provisions therein.

ARTICLE VI LEAP ACCESS RULES

The LEAP program maintains a variety of access requirements for different user audiences.

SECTION 1 LEVELS OF ACCESS TO LEAP

There are currently three levels of access pertaining to the LEAP program:

1. **User Access.** Users in this category are primarily concerned with conducting name checks to identify dangerous individuals, locations and vehicles. They require time sensitive access to basic information, such as all information relating to safety of the officer (subjects dangerous/violent behavior, and prior violent activity associated with an address or vehicle), and pointer information for the officer to get additional information. This query level will also have a very basic capability to combine different query entries such as a person, vehicle and address to determine any simple levels of associations. In addition, approved users in this category will have access to all information at the tactical level, plus all available incident/case information as defined by the contributing agency with all applicable advanced analytical capabilities.
2. **Administrative Access.** Users in this category will be restricted to administrative LEAP functions and they will not have access to any law enforcement information.
3. **Security Access.** Users in this category will have access to the information considered under Levels 1 and 2 plus restricted functionality related to the management of audit and logging information files.

SECTION 2 USER ACCESS

User access provides all participating agencies with the ability to conduct checks to identify dangerous individuals (by name, alias, descriptions, etc.), including addresses, vehicles and events associated with criminal related activity. The resulting messages provide all participants with the ability to have time sensitive access to law enforcement information, beyond basic wants or warrants, to include past law enforcement contacts and behavior or activities that were deemed to be dangerous or violent in nature, or any information that would provide for the tactical safety of any officer making queries of the system. This

access level also provides a pointer directing the user or officer to get additional information about subjects of prior investigations from other participating agencies. It will be the responsibility of the requesting officer or agency, once having accessed the LEAP program, to contact the agency that entered the information and obtain permission from that agency to utilize that data in its entirety.

At this level of access the originating agency will have the responsibility/discretion to either release law enforcement information to the requesting agency or deny access to that agency.

Approved users are also enabled with investigative/analytical capabilities that provide an authorized individual access to advanced analytical tools to conduct investigative analysis, crime problem studies, strategic evaluations, executive briefs, or the development of products based on the analysis of the combination of law enforcement information from all participating law enforcement agencies utilizing the LEAP program.

The investigative/analytical query and resulting messages will enable the user to access more detailed information to include the ability to “drill down” from a name, place, event or other identified entity to the actual documents or records from all participating agencies. This capability will enable the authorized user to examine documents, forms or other information to include structured and unstructured text and data fields to conduct free text analysis with free text entry queries in an unrestricted manner across all data sources. The user will have the ability to conduct a full analysis of all information obtained as a result of the query, utilizing embedded tools utilized by the LEAP program. The message received by the user will allow the user to fully analyze the links and associations made through the embedded analytical software, and to allow the user to examine the original documents and associations within those documents as a result of developed links and searches.

Access to the LEAP analytical functions, to include all levels of available participating agency information contained within the system, or any other analytical capability of the system will be unrestricted and fully available to users.

There will be no “classified information” contained in the LEAP program but will contain “law-enforcement sensitive” data.

SECTION 3 ADMINISTRATIVE ACCESS

Administrative access provides an authorized individual access to the System Administration screens that are used to manage users and administrator accounts. There are several administrator access levels, the super user level, the system administrator level and the agency administrator level, each of which can only be accessed by designated administrative users based on their roles. At this access level administrators can find an existing user, add new users, edit user information, establish or change user rights, and disable or delete a user account. Each administrative access level addresses the following functionalities:

1. Super-User Administrators are responsible for assigning the administrative and security access privileges to all users at all levels;
2. System Administrators are responsible for assigning other system administrative privileges as well as assigning all agency administrative access;
3. Agency Administrators are responsible for assigning user privileges within their individual agencies.
4. Each level can also manage administrator accounts but only for administrators at the same administrative level or below.

The personnel with administrative level access will not have general access to the Security or User screens. LEAP users will not have access to the administrative functions or screens.

SECTION 4 SECURITY ACCESS

Security access provides an authorized individual access to the LEAP program security screens which are used to manage and produce audits and monitor the system use to ensure appropriate security is being maintained. Any transaction that involves users in the LEAP program will generate an audit record. Audit logs allow system management to

monitor use of the system and to investigate any activity to determine if it is in compliance with legal and administrative requirements governing LEAP.

Security and audit logs will describe what type of action has occurred within the system, which user and user system or agency was involved, and the date and time of the action. The log identifies the kind of action that was taken but does not store the results of the action. The types of actions that generate audit records include failed login, login, logout and each of the query and analytical commands employed by a user during his/her session.

Access to audit logs is determined as part of the establishment of user privileges. The type of access can also be confined to the system or agency levels. Super Users will not have security access privileges for any system. The position of system administrator and security administrator will not be held by the same person.

The personnel with security level access will not have access to the Administrative functions or screens for the system. Administrative users will not be able to access the Security functions or screens for the system.

SECTION 5 INFORMATION ENTRY

For the LEAP program, the mode of information entry is accomplished through access to the originating agency's data, information or other records source. Each of the participating agencies of the LEAP program will normally utilize either a direct data transport link between the agency's record management system or a front porch (data-mart). Agencies may also utilize other means of transporting data to the data center such as data extracts, back-ups, and manual loads, at the discretion of the participating agency. The direct link will be utilized for updating the LEAP program on a regular scheduled or real-time basis.

In the front porch mode, an electronic data transfer will occur on an acceptable schedule from the originating agency's records management system to the front porch then to the LEAP data center facility. Only that information agreed upon by the originating agency will be made available for transfer. The technology utilized for this mode of transfer will not allow for access into the originating agency's record management system, but will only allow for the one-way transfer from the originating agency to the LEAP data warehouse.

SECTION 6 INFORMATION MODIFICATION

Data and information collected in the LEAP program can only be changed by the originating agency and only by changes made to the original data source which will subsequently be reflected in the LEAP program automatically upon the next regularly scheduled update of the LEAP program by the originating agency. Updates are scheduled as frequently as technologically possible by the originating agency, but no less frequently than once every 24 hours.

SECTION 7 INFORMATION PURGES / CANCELLATION

The purpose of a purge or cancellation is to remove an entire law enforcement record or supplemental record(s) from any originating agency's files. When any record is canceled, all supplemental records appended to it will also be automatically canceled. A record may be canceled ONLY by the agency that entered the record. However, approved agency data integrity staff may request cancellation of a record in the LEAP data center when a serious error is detected with immediate notification made to the originating agency. A record should be immediately canceled by the originating agency when it is determined to contain fatal errors or is ordered purged by a judicial order.

SECTION 8 ALERTS

The purpose of an alert message is for a user to save any query and request that it seek new information to the query from all data sources in the LEAP program. When new information that meets the conditions of the query is identified, an email alert is sent to the user who constructed the query. A query might be of interest to law enforcement for any approved reason including wanted, armed and dangerous, wanted for questioning, a known terrorist, if stopped - notify, etc.

An alert message may be transmitted back to the originating agency's representative by a reverse notification through the LEAP program when the alert subject has been contacted or the activity has taken place. It will be the sole responsibility of the originating agency's representative who entered the alert, or the originating agency's Administrative Officer or designated representative to the Advisory Committee, to immediately remove the alert.

SECTION 9 ERROR MESSAGES

A project approved and established error message advises of an error in the LEAP program for all system transactions.

SECTION 10 ADMINISTRATIVE MESSAGES

Administrative messages are utilized to inform users of the LEAP program status and generally appears on the splash screen of the portal prior to a user entering the analytical section of the LEAP program.

- 1. A message will be transmitted when the LEAP program is going out of service. The time the system is going out of service is entered as applicable, and the reason, e.g., OUT OF SERVICE TODAY FOR FILE MAINTENANCE.**
- 2. A message will also be transmitted to notify users when new data sources or new agencies have begun contributing their data or when new tools become available.**

All administrative messages will be received by all participating agency computer devices regardless of the level of participation in the LEAP program.

ARTICLE VIII QUALITY CONTROL

The LEAP program will maintain a level of quality control over the network system and the data collected from agencies and delivered to users in a way to insure its reliability for use in criminal justice analysis and investigations.

SECTION 1 MAINTAINING NETWORK INTEGRITY

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the originating agency.

1. Security:

Security standards are documented in the LEAP Security Policy, resulting in LEAP being CJIS certified in January 2008 by the Texas Department of Public Safety on behalf of the FBI. The LEAP Security Policy contains documents on personnel, physical and technical security, user authorization and authentication, as well as information on dissemination and utilization of LEAP data.

2. Audit:

The CSC shall establish an audit procedure for users, and agencies to ensure compliance with LEAP Advisory Committee Security Policy and established regulations. In addition to audits conducted, the LEAP program shall be independently audited at least once every two years (or other acceptable period designated by the Advisory Committee), by an independent audit staff. The objective of this audit is to verify adherence to policy and regulations and is termed a compliance audit. In order to assist in this audit, each user will respond to a pre-audit questionnaire which will serve as the audit guideline. A compliance audit by individual, agency or the entire system may be conducted on a more frequent basis should it be necessary due to failure to meet standards of compliance.

Such compliance audits shall cover the following areas:

- a. Accuracy: Any LEAP program entry should contain only data that is deemed correct by the contributing agency. In addition agencies should maintain necessary audit documentation for the prescribed period of time as required by established**

Advisory Committee policy. They should also ensure that audit documentation is available from all users accessing LEAP.

- b. Completeness: Information contained in a LEAP program entry from a law enforcement record to be disseminated into the system will contain all of the available records that can be legally disseminated by the contributing agency, and will be comprised of all the pertinent available information.**
- c. Timeliness: Exposure, modification, update, and removal of information are completed as soon as possible after information is available and information is processed and transmitted in accordance with established standards.**
- d. Security: All organizations participating in the LEAP program will comply with the Security Policy adopted by the Advisory Committee. It is the responsibility of each participating organization to protect its sensitive law enforcement information against unauthorized access, ensuring confidentiality of the information in accordance with all laws, policy, regulations, and standards.**
- e. Dissemination: All information will be released in accordance with applicable laws, regulations, and policies established by the Advisory Committee. An audit capability will be maintained in the system to track the access of information by participating agencies and users to ensure access by only the appropriate authorized person. In addition, the CSC should ensure that documentation based on the scheduled security audits is available to assist in biennial audits.**

3. Training:

The CSC or their designees, in conjunction with other Advisory Committee approved entities will:

- a. Train, and affirm the proficiency of system (equipment) operators in order to assure compliance with Security Policy and Advisory Committee policies and regulations;**
- b. Biennially, reaffirm the proficiency of system (equipment) operators in order to assure compliance with Advisory Committee Security Policy;**
- c. Maintain records of all training;**

- d. **Initially provide all law enforcement personnel with basic training to ensure effective use of the LEAP program and compliance with Security Policy and Advisory Committee policies and regulations;**
- e. **Make available appropriate training on the LEAP program for criminal analysts and criminal justice practitioners other than sworn personnel;**
- f. **Provide all participating law enforcement agencies and other practitioners with continuing access to information;**
- g. **Provide peer-level training on LEAP program use, regulations, policy, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers; and**
- h. **Annually review all curricula for relevancy and effectiveness.**

SECTION 2 MAINTAINING THE INTEGRITY OF LEAP RECORDS

Agencies that participate in and contribute records to the LEAP program are responsible for their accuracy, timeliness, and completeness. The integrity of the data in LEAP will be maintained through: 1) automatic normalization upon retrieval, which rejects certain common types of errors in data entered with immediate notification to the originating agency; 2) automatic refresh of data which will provide for purging of records; 3) quality control checks by the appropriate entities, and 4) periodic crosschecks of all records on file for validation by the agencies that entered it. This section addresses quality control and validation procedures.

1. Accuracy:

The accuracy of the law enforcement records is an integral part of the LEAP program. The accuracy of a record is the sole responsibility of the originating agency.

2. Timeliness:

Records must be contributed promptly to ensure maximum system effectiveness. Prompt availability is defined as regular updating of the data exposed to the LEAP program by participating agencies of all law enforcement data, as established by the Advisory Committee.

- a. **Timely modification of a record is that which occurs as soon as possible following the detection of erroneous data in an existing law enforcement record and as soon as possible following the exposure of data to the system.**

- b. **Timely contribution of a modification occurs as soon as reasonably possible once the record in question has been retrieved from the originating agency.**
- c. **Timely removal from the system requires immediate removal of the record once the originating agency has documentation that the information is not accurate or contains false information or should be removed or purged from exposure to the system as a result of any other action.**

3. Completeness:

Complete records (defined as all of the available records that can be legally disseminated by the contributing agency contained within the contributing agency RMS) which include all law enforcement information that was available with reference to any entity at the time of contribution to the system. Validation should include a review of whether additional information which is missing from the original entry that could be added has become available for the record.

SECTION 3 QUALITY CONTROL

CSC personnel will periodically check records contributed for accuracy. All errors discovered by or reported to the CSC in the records are classified as serious errors. This classification determines that immediate action must be taken by the originating agency.

In connection with maintaining the integrity of the records, each agency should develop and maintain stringent quality control procedures to ensure that all records contributed to the LEAP

System is kept accurate, complete, and up-to-date. Upon notification of a case of serious error, the originating agency will correct the record and the LEAP program will automatically retrieve any modified records reflecting accurate information to be included in the LEAP program.

Assumption of a limited responsibility for the cancellation of participating agencies' entries, in connection with the foregoing quality control procedures, does not make the Advisory Committee or its designated representatives the guarantor of the accuracy of LEAP program records. The originating agency retains complete responsibility for the

accuracy, completeness, and current status of its law enforcement records contributed to the LEAP program.

SECTION 4 VALIDATION

A validation request obliges the originating agency to confirm that the record is complete and accurate. Validation is accomplished by reviewing the data contributed to the LEAP program and supporting documents in consultation with the appropriate officer, agent, prosecutor, court, or other originating entity. In the event the validation is unsuccessful the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the LEAP program.

The originating agency will receive requests for records to be validated and will in turn provide validation to the approved LEAP user as appropriate in a timely manner, as established by the Advisory Committee. Validation procedures will be formalized by the Advisory Committee and copies of these procedures must be on file for review during an audit. In addition, documentation and validation efforts must be maintained for review during such audit.

Validation certification means that:

1. The records obtained through the query have been reviewed and validated by the originating agencies;
2. The records which are no longer current have been removed from the LEAP program and all records remaining in the system are valid and active;
3. Records contain all available information; and
4. The information contained in each of the records is accurate.

SECTION 5 RETENTION OF LEAP SEARCH RESULTS

When an operational inquiry on an individual, vehicle, address or event yields a valid positive response, any produced printout showing the inquiry and the record(s) on file in LEAP may not be retained in the agency files without the authority of the originating agency, and will not be intended for use in directly documenting probable cause. Any documentation placed in an agency's records will be marked accordingly and maintained as a permanent part of those records.

When a LEAP inquiry yields positive investigative information that must be printed or reproduced in any manner, or maintained as an official record within an agency, the employee or analyst (if different from the requesting law enforcement officer), making the inquiry should note on the terminal-produced records precisely:

- 1. How the information was obtained;**
- 2. When the information was obtained (date/time stamp recommended);**
- 3. Who the information was produced for;**
- 4. Initial and date all documents; and**
- 5. Forward the documentation to the appropriate officer or agency which may be retained in the inquiring agency's investigative case file.**

SECTION 6 FILE REORGANIZATION AND PURGE SCHEDULE

During the dynamic or regularly scheduled data updates retrieved from the originating agencies' RMS' through the front porch, records that require purging or modification will be automatically accomplished by an established LEAP program data purge or modification procedure.

ARTICLE IX CJIS SECURITY SUB-COMMITTEE

The LEAP Advisory Committee shall maintain a CJIS Security Sub-Committee (CSC) to monitor and otherwise be aware of and to be the primary contact for the Advisory Committee on the reporting of potential and/or actual violations or allegations of violations of improper or otherwise unwarranted access to, use and dissemination of electronic information maintained by LEAP.

SECTION 1 THE CJIS SECURITY SUB-COMMITTEE

The initial review procedures by the CSC will be determined based on how the alleged wrongdoing is discovered.

In matters that are referred directly to the CSC through annual audit reports, Security Administrators, or third party complaints:

1. The CSC will conduct a review of any reported incident of alleged misuse or abuse of access to the LEAP program or of information obtained through the LEAP program by an employee of any user agency.
2. A determination will be made by the CSC whether the allegations are administrative or criminal in nature.
3. Once issues are identified, the CSC will refer the initial information to the affected user agency. A recommendation will be made that the agency conducts at least an administrative review of the issue.
4. Criminal allegations of illegal access to the LEAP program or illegal use of information obtained from the LEAP program will be referred directly to the affected agency **and** to the prosecuting attorney's office with the appropriate jurisdiction. A recommendation will also be made to the affected agency for administrative action to be taken.

In matters discovered through internal processes engaged in by the participating agency such as internal system audits, inadvertent discovery, third party complaints, or other means:

1. The employing user agency of the accused employee will initiate its own internal investigation within the agency. The employing agency will notify the CSC of the nature of the allegation and if the allegation is criminal or administrative in nature.

2. At the conclusion of any investigation conducted by the user agency the results of any investigation will be made known to the CSC. Investigative results will not include any information or details of the investigation or any information prohibited from being disseminated by law, policy, etc.

In matters reported to the CSC or any other Advisory Committee member by a LEAP participating agency, the referral would be made to both the user agency in question and the CSC by the participating agency.

1. A recommendation will be made by the CSC that the affected agency conducts an internal investigation.
2. The Executive of the affected department shall provide the CSC or Chairman of the Advisory Committee with information of the complaint and with an estimate as to when the investigation will be complete.

No Executive will give up his/her right to investigate internal allegations against his/her own employees.
--

Responsibilities of the CSC are limited to the review of reported incidents. The CSC does not conduct investigations. The CSC is charged with:

1. being aware of any misuse of the LEAP program or misuse of information obtained through access to the LEAP program;
2. receiving allegations of improper access to the LEAP program or misuse of information obtained from the LEAP program;
3. alerting the accused person's employer of the information surrounding the improper activity;
4. being aware of the outcome of the employee's agency investigation;
5. reporting the entire incident to the Advisory Committee. All incidents that affect the integrity of the LEAP program are reported directly to the Advisory Committee.

The responsibility of the Advisory Committee, as a body, is to consider the facts as presented by the CSC and possibly the Agency affected by the incident. The Advisory Committee will consider only those facts as they specifically pertain to the LEAP information sharing system. As a result of the deliberation of the Advisory Committee, a decision will be made binding on all parties involved. Sanctions recommended must be

approved by a unanimous vote of the Advisory Committee (less the affected agency if such agency Executive is a member of the Advisory Committee).

Any sanctions approved by the Advisory Committee must be:

- 1. In compliance with the current Memorandum of Understanding;**
- 2. In compliance with the sanctioned and agreed upon Rules as defined in the Manual of Administrative and Operational Guidelines;**
- 3. In full compliance with all applicable laws and ordinances;**

Sanctions agreed upon by the Advisory Committee will also be:

- 1. Imposed for corrective action only;**
- 2. Designed to protect the LEAP program;**
- 3. Demonstrate “due diligence” on the part of the Advisory Committee in managing LEAP;**
- 4. Specific in nature, and focused only on the related issue;**
- 5. Have a compliance component;**
- 6. Be issued with a precedent in mind.**

SECTION 2 LEAP CJIS SECURITY PROCEDURES

1. Reporting Allegations

Minor issues of negligence that are reported either to the agency or directly to the CSC, will be reviewed by the CSC with the results of the review forwarded to the affected agency with recommendations for a complete review. In minor matters, at the discretion of the CSC, a corrective recommendation may be included in the review prepared by the CSC.

Reportable allegations – any suspected or confirmed improper access to the LEAP program or improper use of information obtained from the electronic warehouse will be reported to the CSC or Advisory Committee in writing, in person or via standard electronic means.

Any allegation that any member of the CSC or Advisory Committee becomes aware of will be recorded. The CSC will maintain the information and a copy will be shared with the affected employees employing agency.

As a result of any referred report, user agencies will conduct at least a preliminary administrative inquiry or investigation into any LEAP related incident. The affected user agency will conduct the investigation of the incident through established internal processes. Investigations are conducted by the affected user agency or by an alternate agency as identified by the Executive of the affected user agency and not by the CSC. Criminal allegations of misconduct will be referred to the appropriate prosecutor with jurisdiction.

All LEAP related incident investigative findings resulting from information given to the affected employee's agency by LEAP shall be reviewed by the CSC. The review will be at the level provided by law and will not involve the disclosure of any information not allowed by federal, state, county or municipal laws.

To ensure that privacy is protected and no personnel records are being disclosed, it is suggested that the incident review of the investigation between the CSC and the user agency investigators consist of a verbal briefing.

A synopsis of the actions taken by the user agency will be presented to CSC. Based on a review of the investigation conducted by the user agency, a recommendation for action will be made by the CSC to the Advisory Committee.

Any actions recommended by the CSC will be limited to those sanctions approved and adopted by the Advisory Committee and made part of the approved LEAP Manual of Administrative and Operational Guidelines.

If the Advisory Committee determines the user agency did not handle the investigation or any resultant disciplinary action in a manner that maintains the integrity of and good faith in LEAP, the Advisory Committee may take action and impose sanctions on the user agency. Such actions by the Advisory Committee will require a unanimous concurrence of all Advisory Committee members (less the affected agency if represented on the Advisory Committee). Any actions will be limited to those provided in the Manual of Administrative

and Operational Guidelines or the data sharing MOU between the agency and the Advisory Committee.

Any documents produced as a result of the inquiry or investigation will be made a part of the Advisory Committee's official records and maintained in a secure location under the administrative protection of a Council of Governments. Consideration for the location and storage of Advisory Committee documents related to incident reports and investigations should be in such a manner as to protect the privacy of those individuals involved. Upon location of an adequate facility and upon unanimous approval of the Advisory Committee, the facility can be adopted as the permanent storage facility for all records regardless of the change in Advisory Committee Chairs.

Sanctions to be considered by the CSC for any action related to an incident involving the LEAP program are limited to those designated in the Sanctions portion of the Manual of Administrative and Operational Guidelines. At the discretion of the Advisory Committee, and by unanimous consensus, sanctions may be added or modified as appropriate. In all instances, an individual or agency is presumed innocent until evidence shows otherwise.

- a. An individual accused of serious misconduct, misuse or negligence with the LEAP program should immediately have system privileges suspended until the conclusion of the investigation.**
 - b. In the case of an agency, in general, that clearly allows routine violations of the adopted rules or security requirements, or fails to correct identified serious problems within their agency, the agency should have all access suspended until the issue is resolved by the Advisory Committee.**
- 2. Addressing allegations of misconduct If internal misconduct of an employee is discovered by an agency:**
 - a. The agency head will report any allegations of LEAP program misconduct, misuse or negligence by an employee or the agency to the Advisory Committee or the CJIS Security Sub-Committee as soon as possible;**

- b. **All official investigations of allegations against an individual will be conducted by the agency in which the accused is a member;**
- c. **Investigations of allegations against the agency will be conducted by the Committee or it's official representative;**
- d. **Investigations will be considered an administrative complaint and will be conducted in the same manner (i.e., according to agency policy) as other allegations of misconduct within that agency;**
- e. **If criminal conduct is discovered the internal investigation will immediately cease and the investigating body's (Internal Affairs or Professional Standards) Commander will report to the agency head that suspected criminal behavior has been discovered.**
 - i **The agency head, or his representative, will brief the locality's District Attorney's Office (DA) on the alleged criminal behavior, and if the allegations rise to the level of "probable cause" of criminal conduct and a prosecution decision is made, the agency head will turn the investigation over to the appropriate departmental criminal investigators;**
 - ii **The administrative investigation will closely follow the criminal investigation, only interviewing witnesses and gathering evidence after the criminal investigators have completed those phases of the investigation so as not to jeopardize the criminal investigation.**
- f. **Criminal investigations normally target violations of criminal law while administrative investigations target administrative policy/rule violations. Therefore there is a necessity for two separate and distinct levels of investigations to satisfy the needs of future criminal or administrative procedures or hearings.**

In all instances every precaution will be taken to protect the privacy and legal rights of any affected or accused party.

- i The CSC will submit a written report to the Advisory Committee and give a verbal briefing of the allegations, investigation and actions taken by the agency head;**
 - ii The Committee will then vote to accept the decision of the agency head in the matter, reject the decision and, if necessary, impose sanctions on the individual or agency, or call for additional information before deciding;**
 - iii The matter will be made a part of the minutes and official records of the Advisory Committee meeting.**
- 3. If misconduct is discovered by a member agency or reported to the Committee:**
 - a. If LEAP program misconduct, misuse or negligence is alleged to have been committed by an employee of a member agency, the Committee Chairman will contact the accused agency head to follow the procedures outlined herein for internal investigations;**
 - b. If LEAP program misconduct, misuse or negligence is alleged to have been committed by an agency in general, or an individual directly employed by a vendor or another individual not directly employed by a participating agency, the CSC will be responsible for delegating the investigation to the appropriate investigative body;**
 - c. In the case of b., (above), the Advisory Committee or the Executive Committee will convene the CSC to review all available information prior to the start of the investigation for full concurrence;**
 - d. When the CSC requests an investigation, it will be the responsibility of the CSC with the concurrence of the Advisory Committee to appropriately monitor that investigative matter;**
 - e. The investigating agency (Internal Affairs or Professional Standards) Commander or designee of the chief law enforcement executive will directly oversee or conduct the investigation;**

- i If criminal conduct is discovered the investigation will cease and the investigating commander will report same to the agency head and the CSC;**
- ii The CSC will immediately contact the Advisory Committee, notifying them of the appearance of criminal conduct;**
- iii The Committee will then convene and a decision will be made on how to further proceed;**
- iv At a minimum, the Committee will recommend contact with the DA's Office in the jurisdiction in which the alleged criminal conduct was thought to have occurred. The investigators will brief the DA, as well as receive a prosecution decision if the allegations rise to the level of "probable cause" of criminal conduct;**
- v If the locality's DA makes a decision to prosecute, the affected agency will turn the investigation over to the agency's internal or criminal investigators;**
- vi In the case of allegations of criminal conduct by an agency, the Committee will turn the matter over to the appropriate investigative jurisdiction.**
 - a) The administrative investigation will closely follow the criminal investigation, only interviewing witnesses and gathering evidence after the criminal investigators have completed that phase of the investigation;**
 - b) The investigating body's commander will complete a report at the conclusion of the investigation and present it to the CSC;**
 - c) The CSC decide to take the committee recommendation to the Advisory Committee or ask for additional investigation or clarification;**
 - d) The CSC will present the findings to the Advisory Committee with recommendations for appropriate sanctions;**
 - e) If the allegations are determined to be substantiated either as criminal or administrative issues with respect to the LEAP program, the Committee could impose administrative sanctions, as it deems appropriate.**
 - f) Administrative sanctions must be approved by a unanimous vote of the Committee (less the affected Agency).**

SECTION 3 INTRODUCTION TO LEAP SANCTIONS

Purging of an agency's investigative records and discontinuance of LEAP program access for an agency are the two ultimate sanctions available to the Advisory Committee for enforcement of LEAP program policy and procedure. This presumes prosecution for violations of Federal, State, County or Municipal laws and ordinances would normally be directed toward an individual rather than toward an agency.

1. Considerations:

a. An up-to-date MOU and Advisory Committee approved Manual of Administrative and Operational Guidelines should be on file with the Advisory Committee and the administrative representative for each participating agency. They should include a reference to the sanctions that could be imposed for failure to comply with the Rules, Security Policy as well as criminal breaches.

b. Specific references should include but are not limited to:

- i Failure to react properly to error notices**
- ii Failure to react properly to information confirmation requests**
- iii Failure to provide complete entries/modifications/removals promptly**
- iv Failure to provide data updates**
- v Failure to validate information**
- vi Failure to assure security of equipment and data**
- vii Contribution of invalid or nonqualified records**
- viii Criminal misconduct**

2. A special audit of a participating agency with access will be part of the sanction package upon request of the Advisory Committee.

In matters involving an agency participating in a substandard manner flagging that agency's records will be an option of the Committee. If the committee needs to meet to discuss and determine sanctions it can be done via audio or video conference.

Deadlines will be imposed on compliance with corrective action notices.

SECTION 4 SANCTIONS

Specific sanctions directed to participating agencies by the Advisory Committee for administrative issues are commenced by the transmittal of a message by the CJIS Security Sub-Committee on behalf of the Advisory Committee in writing to the participating agency for all noted issues and/or errors.

When the Advisory Committee is notified of possible criminal activity, the Chair will immediately notify the highest ranking executive of the affected agency. The next business day, the CJIS Security Sub Committee will be notified and convene via audio conference. The CJIS Security Sub Committee will terminate access to LEAP for the affected agency until the issue has been resolved by the CSC.

The Advisory Committee, with assistance of its sponsors, is to maintain a copy of these messages for follow-up, and as a matter of record for a period consistent with the Texas Records Retention Schedule.

In matters where agencies have been notified of repeated substandard practices over consecutive years, the agencies will be asked to bring their practices up to acceptable standards.

A letter of request for compliance will ask the agency to respond to noted substandard practices and describe improvements in the following areas, including but not limited to:

- 1. Untimeliness;**
- 2. Inaccuracy;**
- 3. Incompleteness;**
- 4. Unsatisfactory record quality;**
- 5. Unsatisfactory validation;**
- 6. Non-criminal misuse of system notice resulting from audit (with recommended time-frame for corrective action);**

After receipt of a letter of request for compliance, serious failure of a participating agency to ensure satisfactory policy compliance will result in the delivery of a written letter of intent to remove the participating agency from the system until deficiencies are corrected.

Removal from the system includes the removal of access to all agency records and discontinuance of service pending reinstatement approval by the Advisory Committee.

SECTION 5 REINSTATEMENT

Upon satisfactory proof that the offending participating agency has corrected its deficiencies, with verification by the CJIS Security Sub Committee, the Advisory Committee may reinstate the agency.

Specific sanctions directed to participating personnel by the Advisory Committee for administrative infractions or criminal acts are recommended to include:

- 1. In non-criminal matters, a letter will be transmitted by the CJIS Security Sub Committee on behalf of the Advisory Committee in writing to the participating agency. The Advisory Committee sponsors are to maintain a copy of these messages for follow-up, and as a matter of record for a period consistent with the Texas Records Retention Schedule.**

- 2. In all matters where an administrative personnel issue has been brought to the attention of the CJIS Security sub Committee or the Advisory Committee, with regard to any user of the system, sanctions could be recommended or imposed by the Advisory Committee. In all instances the Advisory Committee reserves the right to impose or waive sanctions at their discretion in the following manner:**
 - a. Verbal request to the user's agency for counseling on compliance;**
 - b. Written request to the user's agency for counseling on compliance;**
 - c. Written recommendation for retraining;**
 - d. Written notification for repeated non-compliance with a recommendation for internal performance based action;**

- e. **Suspension of user privileges for a period agreed upon as appropriate by the Advisory Committee;**
 - f. **Permanent revocation of user privileges as agreed upon by the Advisory Committee.**
- 3. In all matters where there are allegations of criminal misconduct involving the use of the LEAP program, user privileges will be immediately suspended until the matter is resolved to the satisfaction of the user's agency and the Advisory Committee.**
- a. **Any allegations of criminal misconduct will be referred to and addressed by the appropriate investigative agency and/or prosecutor, as indicated herein.**
 - b. **Criminal prosecution of any user for actions related to the use of the LEAP program will result in permanent suspension of access to the system by that user.**

Recommended procedures for addressing any incident involving LEAP users brought to the attention of the CJIS Security Sub Committee, the Advisory Committee, or participating agency are established in Article IX.

ARTICLE X DEFINITIONS

Administrator – The LEAP Advisory Committee

Sponsor – North Central Texas Council of Governments (NCTCOG)

Gatekeeper – Third party organization performing its duties of auditing LEAP usage, and communicating with NCTCOG, LEAP Advisory Committee and those law enforcement agencies participating in LEAP

Gateway – The Internet enabled application developed to support vetting LEAP users, administer access to LEAP, and provide usage reports

Administration of Criminal Justice – The detection, apprehension, detention, pretrial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history information; and criminal justice employment.

Authorized User – An individual designated by an agency head and authorized by the Administrator for direct access to system.

Direct Access – The action of an individual authorized user to gain direct computer access to LEAP.

Criminal Justice Agency – A federal, state, local or tribal entity that is engaged in the administration of criminal justice under a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice.

Indirect Access – The action of an individual, who is not an authorized user, to gain indirect access to system through an authorized user based on a right and/or a need to know.

Information Quality – The validity, accuracy, timeliness, completeness, relevancy importance, and reliability of information supporting a record.

Local Entity – An agency or other entity of a political subdivision of Texas, including a city or county. The term includes a task force, law enforcement agency of a school district or institution of higher education, whether public or private, or other local entity that is engaged in the administration of criminal justice under a statute or executive order.

Memorandum of Understanding - An agreement executed under these policies and procedures established by the LEAP Advisory Committee and the Participating Agency.

Need to Know – The necessity to obtain or receive criminal intelligence information in the performance of an official duty of an authorized user or responsibility for a criminal justice agency.

Participating Agency – A criminal justice agency which has access to LEAP services and has completed a LEAP Memorandum of Understanding. The term may include an entity that functions as a regional sponsor.

Right to Know – The legal authority to obtain or receive criminal intelligence information under a court order, statute, or decisional law.

User Agreement – An agreement executed as a Memorandum of Understanding under these policies and procedures by the Authorized User.

ARTICLE XI LEAP USER AGREEMENT

LAW ENFORCEMENT ANALYSIS PORTAL USER AGREEMENT

Introduction:

The Law Enforcement Analysis Portal (LEAP) operates under the governance of the LEAP Advisory Committee with the sponsorship of the North Central Texas Council of Governments (NCTCOG) and the non-criminal justice agencies contracting to support certain functions for NCTCOG, as the service providers, and the criminal justice agencies, as both service providers and service users.

You have requested, or your agency has requested on your behalf, computer access to LEAP.

Before this access is granted, you must agree to abide by usage and access policies and to use your LEAP account in an acceptable, ethical and legal manner.

Privileges and Responsibilities as a LEAP User:

As a user of the LEAP program, I will adhere to the following security rules:

- 1. I will use LEAP only for the administration of criminal justice.**
 - a. I will respect the confidentiality and privacy of individuals whose records I may access.**
 - b. I will observe any ethical restrictions that apply to data to which I have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information.**
 - c. I am forbidden to access or use any LEAP data for my own personal gain, or profit, or the personal gain or profit of others, or to satisfy my personal curiosity.**
- 2. I agree to review and complete the on-line tutorial before accessing LEAP.**
- 3. I know that I will be issued a user identifier (User ID) and a password to authenticate my LEAP account. After receiving them:**

- a. **I understand that my LEAP computer account is assigned to me alone and is not to be shared with anyone, including co-workers, trainers, or computer technicians. I will not allow anyone else to have or use my password.**
 - b. **If I know that my password is compromised, I will report the compromise to my agencies' LEAP Point of Contact (POC) and to the LEAP secure access representative.**
 - c. **I am responsible for all activity that occurs on my individual account once my password has been used to log on access to LEAP.**
 - d. **I will ensure that my password is changed at least twice a year or if compromised, whichever is sooner.**
 - e. **I will not store my password on any processor, microcomputer, personal digital assistant (PDA, such as a Palm Pilot or Blackberry), personal electronic device, or on any magnetic or electronic media.**
 - f. **I will never leave my LEAP session unattended while I am logged on.**
 - g. **I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else for the purpose of access to LEAP.**
 - h. **I will not connect any personal information technology equipment (for example, PDAs, personal computers, or digitally enable devices) to the terminal I am using to access LEAP for the purpose of downloading LEAP data.**
 - i. **If I observe anything on the system I am using that indicates inadequate security, I will immediately notify my agency's LEAP POC. I know what constitutes a security incident and know that I must immediately report any such incidents to my agency LEAP POC.**
4. **I may pass along information I obtained from LEAP only to other persons who do not have direct access to LEAP and are known by me to be law enforcement or criminal justice personnel.**
 5. **I agree not to use the resources of LEAP in such a way that the work of other users, the integrity of the system, or any stored data may be jeopardized.**

- 6. I agree that if, in the opinion of the LEAP Advisory Committee, my use of the resources contravenes any provision in this agreement, or is in breach of any rules in force for the time being, my access to LEAP will be withdrawn. Any dispute arising from such action, or arising from other provisions of this agreement will be conducted under the appropriate disputes and appeals procedure within the LEAP Advisory Committee and agreement with the providers of information comprising the LEAP.**
- 7. I understand that the LEAP Advisory Committee nor its sponsors accepts no responsibility for the malfunctioning of any equipment or software, nor failure in security or integrity of any stored data.**
- 8. I understand that no claim shall be made against the LEAP Advisory Committee nor its sponsors, its employees, or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act or neglect of the LEAP Advisory Committee nor its sponsors, its employees, or agents.**
- 9. I know that my actions as a LEAP user can greatly affect the security of the LEAP program and that my signature on this agreement indicates that I understand my responsibility as a LEAP user requires that I adhere to regulatory guidance.**

If you choose not to accept these standards of behavior, you will be denied access to LEAP. Violators of these standards will be reported to their respective agency head.

Acknowledgment and Acceptance:

I acknowledge and accept the responsibilities as set out in this agreement. I acknowledge that these responsibilities have been developed and approved by the LEAP program users and providers of information to LEAP in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in LEAP. I further acknowledge and accept that my failure to comply with these responsibilities will subject my access to various sanctions as approved by LEAP Advisory Committee. These sanctions may include termination of my access to LEAP.

I understand and agree to abide by the conditions outlined above.

The above User Agreement is encountered as a click-through license the first time that a LEAP user is enabled and signs on to the system. The User Agreement is available at all times from the main splash screen once a user signs on to the LEAP program but the user need only read and execute the click-through license on the first sign-on.

ARTICLE XI MISCELLANEOUS PROVISIONS

This Manual of Administrative and Organizational Guidelines may only be modified by the LEAP Advisory Committee and may not be modified by the parties to this MAOG without the consent of the LEAP Advisory Committee.

ARTICLE XIII ACKNOWLEDGEMENT

This Manual of Administrative and Operational Guidelines has been received by the undersigned who acknowledges that the agency and its participants who access the LEAP services will abide by the terms and conditions of usage as stipulated.

SPECIAL ATTENTION IS DIRECTED TOWARDS THE TERMS AND CONDITIONS OF ARTICLE IX – OVERSIGHT AND THE SANCTIONS ASSOCIATED WITH MISUSE OF THE LEAP PROGRAM.

Agreed and Acknowledged:

<u>For Agency:</u>		<u>For LEAP Advisory Committee:</u>	
<i>Agency Name</i>		<i>Agency Name</i>	
<i>Signature</i>		<i>Signature</i>	
<i>Printed Name</i>		<i>Printed Name</i>	
<i>Title</i>	<i>Date</i>	<i>Title</i>	<i>Date</i>
	_ / _ / _		_ / _ / _