North Carolina Law Enforcement Information Exchange (LInX)

RULES OF OPERATION

North Carolina LInX - Version 3.0

LInX RULES OF OPERATION

TABLE OF CONTENTS

SECTION 1: What Is the LInX System?

Since September 11, 2001, federal, state, county and municipal law enforcement have experimented with information sharing on an unprecedented level. The LInX initiative has enhanced the flow of law enforcement information between federal, state, county and municipal authorities at the regional level, with a focus on detecting and neutralizing all levels of criminal activity, including terrorism. The effort integrates law enforcement data currently resident in record management systems within agencies or on regional networks and provides query and analytic tools to support officer safety, criminal and terrorism investigations, and crime prevention strategy development. LInX provides law enforcement agencies with near-real time access to investigative reporting from each of the other participating jurisdictions within the region, as well as a capability to apply link analysis and other tools across all the available investigative data.

The LInX System seeks to integrate the collective knowledge of regional law enforcement agencies into a central data warehouse with state-of-the-art analytic tools. This includes collection and integration of all participating agencies' law enforcement information relating to locations, crimes, suspects, associates, arrests, etc. This information will be accessible by all of the participating agencies and originate from the records management systems (RMS), or other data sets found in their operational, case management, or investigative systems, (as discussed herein and in other North Carolina (NC) LInX documentation, the NC LInX System does not contain any law enforcement intelligence information). Through the data warehouse the information from the participating agencies is available to serve as a tactical, analytical, and strategic tool for officers, counterterrorism investigators, criminal investigators, analysts, and agency executive decision makers.

1.1 PROJECT DESCRIPTION

The LInX initiative provides access to the cumulative knowledge of participating area law enforcement agencies in a systematic and ongoing manner to aid development of district counterterrorism and crime strategies providing for collaborative investigations and cooperative information sharing. The LInX system software licenses, hardware and technology concept is fully owned by the U.S. Government, not a private vendor, and as such, is totally controlled and managed by NCIS and its law enforcement partners within each LInX region. The system has been built from commercially available technologies, with appropriate security filters and privacy protection tools, which enable the data warehouse to provide for the access, collection and analysis of federal, state, county and municipal law enforcement records and investigative information.

LInX is comprised of a regional data warehouse for "Sensitive but Unclassified" (SBU) or law enforcement sensitive information. At the discretion, and upon approval of the NC LInX Governance Board, additional law enforcement agencies may be added. In the future the NC LInX Governance Board may also choose to support other agency's efforts to establish a link between the LInX System and a "special task force," "sensitive" or "classified" data sharing environment. The data warehouse uses existing networks to

access and retrieve data and has its own suite of query and analytical applications enabling users to exploit information in the database. Federal information received from all federal records systems made available for inclusion, will be appropriately filtered to remove restricted or classified information such as Federal Grand Jury (6(e)), Title III, financial privacy, or other information that requires special provisions for dissemination.

The LInX System provides access to disparate law enforcement agency investigative data and with use of the data warehouse, is able to generate law enforcement and management reports that can satisfy the needs of four general user groups: executive strategic decision makers, analytical staff, law enforcement patrol or tactical officers, and investigative staff. The system is capable of accessing data to be incorporated within the data warehouse which provides customized reports to satisfy each user group, and is capable of providing scheduled reports as determined by each user group. The disparate data information and reports can/may be formatted for viewing on a Web based browser, as well as through desktop applications including word processors, spreadsheets, and desktop databases such as Access.

1.2 USE OF DATA AND PROBABLE CAUSE

A. The data content of the LInX System may not and 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. A hit alone through the LInX System is not probable cause, but indicates that data, a report or other information exists in the Records Management System (RMS) of an identified participating agency. A positive hit in the LInX System should be considered only one element 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 LInX System is not considered, and should not be used for, "original documentation" for probable cause in support of any court testimony by any participating agency.

B. Correct LInX System procedures, as agreed upon by the NC LInX Governance Board, requires the agency which provided access to (or "owns") the data be contacted by the inquiring user to confirm that the data is accurate and up-to-date. In some circumstances, the hit 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.

For instance, from a confirmation of law enforcement information existing in a participating agency's RMS on an individual or a hit on a vehicle or property, the inquirer must obtain a confirmation directly from the original agency and not utilize the documentation obtained from the LInX System to directly support probable cause, searches, or other activity that would likely lead to testimony. The verification of the information and confirmation of

validity from the originating RMS, regardless of how long it had been in the data warehouse, may be enough cause to take appropriate and reasonable action.

C. Records, such as the Violent Gang, Terrorist Organization, Convicted Person on Supervised Release, Convicted Sexual Offender Registry, Protection Orders and other officer safety or public safety "alerts" included within the LInX System do not require immediate hit confirmation and by their nature are designed to provide law enforcement officers with adequate warning regarding individuals who have had involvement in violent criminal activities or are known to represent potential or immediate danger to the investigative officer and/or the general public.

1.2.1 USE OF DATA EXCEPTION

The data and information NC LInX agencies contribute to the LInX System include arrest and booking photographs provided for use by the participating agencies in conducting investigations. As authorized by the NC LInX Governance Board, in matters deem *exigent* by the NC LInX System users, arrest and booking photographs may be printed from the NC LInX System for the purpose of witness identification through a photo line-up or use as an elimination photograph.

Exigency may vary from cases to case however it should generally be considered a set of circumstances in which the delay necessary to obtain the photographs or materials through other means would create a legal issue regarding detention or would result in the loss of critical evidence which could not be gained by other lawful means. Furthermore the exigency exception shall be in accordance with all federal, state and local laws and shall require documentation of the circumstances in the agency investigative report.

In any circumstances where a photograph is used directly from the LInX System for exigent purposes the user will comply with Section 3.5 "Retention of LInX Search Results" herein, as well as all North Carolina laws and ordinances relating to the use of arrest and booking photos for official investigative purposes and photo line-ups.

1.3 RESPONSIBILITY FOR RECORDS

A. The LInX System consists of information from existing law enforcement RMS' and records must be kept accurate and up-to-date. Agencies that contribute records in the LInX System maintain total control and ownership of those records and are responsible for their accuracy, timeliness, and completeness. To facilitate compliance with the necessity of confirming the hits within the contributing agencies' records management systems, the originating agency must make available at the latest, on a 24-hour basis, or within a reasonable time frame as accepted by the NC LInX Governance Board, (i.e. next business day), confirmation of any hits from the agency's record entries.

B. 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 sponsoring agency of the LInX System, and the NC LInX Governance Board representatives, will maintain the integrity of the data warehouse through:

1. Establishment of an administrative oversight group for the LInX data warehouse for the purpose of insuring the technical integrity of the system;
2. Utilization of the administrative oversight group for the LInX System for monitoring and maintaining data edits and updates from the participating records management systems;
3. Utilization of an administrative position at each user location for quality control checks;
4. Scheduled updates of the data warehouse using the system capability to insure current and accurate up to date information is being maintained within the data warehouse.

C. All participating agencies in the LInX System will be responsible to insure integrity of the data through:

1. Automated edits insuring the identification and elimination of common types of errors in the law enforcement data;
2. Purging of records maintained for a period of time, as prescribed by laws, ordinances, policies and procedures;
3. Quality control checks;
4. Validating access to records (details concerning quality control and validation procedures appear in Section 3 of this document.)

D. The LInX System makes network accessible data and centralized warehoused 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.

E. This document intends to instruct and is designed as NC LInX policy to guide participants in using the LInX System. 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 and integrity of the program, system and the data stored in the data warehouse.

F. All inquiries regarding any specifics about the technical LInX System should be addressed to the LInX sponsoring agency.

G. All inquiries regarding any specifics about the data or information contained in the LInX System should be addressed to the participating LInX agency that owns the information.

1.4 PROJECT DESCRIPTION

A. LInX System participants will include approved municipal, county, state, and federal law enforcement agencies throughout the prescribed region.

B. Law enforcement records will be transported to the data warehouse from an originating agency's RMS. This is accomplished based on the technical capabilities of the agency, and will include direct dynamic data exposure from the RMS of the originating agencies. Direct dynamic data retrieval, as well as periodic data retrieval are conducted in a controlled fashion through the network connecting the LInX System to the exposed data from the RMS of the participating agencies. Retrieval of data by the LInX System into the data warehouse will provide data that will be "tagged" to identify the originating agency for those records. Once retrieved into the LInX data warehouse, data cannot be altered, deleted, or changed in any fashion by any agency. Any changes will be accomplished by a new data retrieval process from the originating agency for which the data is "tagged" or coded.

The LInX System is designed to interface with equipment manufactured by many of the records management system manufacturers through the use of the front porch, and the components are available commercially off the shelf (COTS). Participants are not required to use the same make computer equipment as that used by any other participant. The only requirement is that equipment be able to "communicate" with the network that has been developed for the LInX System.

1.5 POLICY

A. The NC LInX Governance Board, establishes the policies with respect to the philosophy, concept, operational principles and security of the LInX System for the region. In its deliberations, the NC LInX Governance Board, places particular emphasis on the continued compatibility of the LInX System; network security; along with a particular focus on rules, regulations, and procedures to maintain the integrity of LInX System and the records shared over the system.

B. The LInX control and Governance process is composed of two major components, the sponsoring agency working in conjunction with the Executive Managers (functioning as the NC LInX Governance Board), from each participating agency, and the system working groups. The Governance Board is responsible for reviewing policy issues along with appropriate technical and operational issues related to the System and, thereafter, making appropriate recommendations. The NC LInX Governance Board consists of participating federal, state, county and municipal agency executives, and is limited to those agencies actively participating in the LInX System by contributing law enforcement data to the project, which is

made accessible to all parties. The NC LInX Governance Board works through an established Charter, Memorandum of Understanding, rules, policies, etc., established between each participating department or agency, with the agency executive having direct input into the administration and operation of the LInX System with equal stature among peers.

C. The LInX working groups for the region consist of administrative, legal, administrative, operational and technical experts from the participating departments. It is the responsibility of the working groups to recommend policy, procedures and changes for the LInX System in order to enhance its operability and ensure access by all its participants.

1.6 SECURITY

A. There is no federal level legal or policy prohibition against dissemination of information contained in the LInX System, which consists of derivative law enforcement information, which is disseminated only for law-enforcement purposes. If no state, county, or municipal law, ordinance or policy prohibition exists towards the dissemination of information contained in the LInX System, 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. (see Exception for Arrest and Booking Photos, Sections 1.2.1 and 3.5 herein)

B. Information may be withheld from the LInX System 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 sponsoring agency and the NC LInX Governance Board, to be legitimate.

C. A participating agency must assume responsibility for and enforce security with regard to all users within that agency. The responsibilities of the LInX participating agency Governance Board representatives are outlined in Section 4 of this document.

D. LInX 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 System rests with the individual participating agencies. Further information regarding System security can be obtained through a review of the System Security Authorization Agreement (SSAA) for the LInX System, as well as the approved NC LInX System Security Policy (SSP).

E. All federal, state, county and municipal agencies participating in the LInX System are required to adhere to the security guidelines as set forth in the SSP, and in 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).

F. Data contributed to the LInX System 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 LInX 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 LInX System as specified by the established and accepted LInX directives.

G. Information can be obtained from the LInX System both directly and indirectly with direct access through existing terminals to the network or through the indirect dissemination of law enforcement information outside of the agency with specified access to the system. Indirect access or non-network terminal access outside of an agency with direct access to the LInX is *not permitted* without express written permission of the originating agency for the law enforcement data and the full NC LInX Governance Board, established laws and policies will govern the dissemination of the data contained within the LInX System to nonparticipating agencies.

H. Any agency allowing access to the LInX System must insure that the person being granted access to the project 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 in conjunction with rules and policies established by the NC LInX Governance Board.

I. Access to the LInX System by any non-accredited network, system or program must meet the established Security policies and guidelines of the sponsoring agency to include having been fully certified and accredited by a Federal Designated Accrediting Authority.

J. Unauthorized request, use, dissemination or receipt of LInX information other than as specified herein, could result in any level of administrative sanctions, to include civil or criminal proceedings being brought against the agencies and/or individuals involved depending on the seriousness of the offense involved.

1.7 PROJECT DISCIPLINE

A. To help ensure the proper operation of the LInX System, the standards, procedures, formats, policy and criteria mentioned in this document must be strictly followed. In this respect, the NC LInX Governance Board must not only follow the rules set forth, but must also ensure that participating agencies are doing the same. In doing so, the NC LInX Governance Board, will develop and adopt a set of security standards and policies for the project to be complied with by all participating agencies.

B. Complete, accurate, and timely records are essential to ensure the integrity of the LInX System. 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 LInX System is voluntary, delayed entries of records into the LInX System reduces or eliminates the possibility of addressing criminal or potential terrorist activities or having a significant impact on organized criminal problems within the region.

C. Promptness in contributing, modifying, locating, expunging or eliminating records in the system helps keep the data warehouse free of outdated information.

D. The LInX System 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 LInX System must be verified, validated and evaluated along with other facts known to officers, investigators, analysts, and administrators prior to action being initiated.

SECTION 2: LInX ACCESS RULES

Note; the following has application for the LInX data warehouse only, or the front porch network, or both at the discretion of the sponsoring agency, the NC LInX Governance Board and each of the participating agencies.

2.1 QUERY ACCESS

There are currently four levels of access pertaining to the LInX System:

A. Tactical Access. Users in this category are primarily concerned with conducting name, address or vehicle 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 basic pointer information for the officer to get additional information. This query level will also have a very basic capability to combine different disparate query entries such as physical descriptions, fuzzy names, phone numbers, vehicles, addresses and incidents, to determine levels of associations.

B. Investigative/Analytical Access. Approved users in this category will have access to all incident information at the tactical level, plus all available free text investigative case information as defined by the contributing agency with all applicable free text analysis and link analysis capabilities.

C. Administrative Access. Users in this category will be restricted to administrative LInX functions and they should not have access to any law enforcement information considered under Levels 1 and 2.

D. Security Access. Users in this category can have access to the information considered under Levels 1 and 2, plus restricted functionality related to the management of audit and logging information files.

2.2 TACTICAL ACCESS

Tactical access provides all participating agency users with the ability to conduct checks to identify dangerous individuals (by name, alias, descriptions, etc.), including addresses, vehicles and events associated with regional 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 or the general public. 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 data warehouse, to contact the originating agency that entered the information and obtain permission from that agency to utilize that data in its entirety for any activity that could result in court testimony.

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.

2.3 FULL INVESTIGATIVE/ANALYTICAL ACCESS

The investigative/analytical access provides an authorized individual access to 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 LInX System.

The message format provided to the user will initially appear similar to the tactical message available to all participants regardless of access authority. The investigative/analytical query and resulting messages will enable the preapproved user to access more detailed information to include the ability to "drill down" from a name, place, event or other identified entity to accessing 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 approved query, utilizing tools such as (used by name for example only) i2 Analyst Notebook, Visual Analytics or other analytical software capabilities available for use by the data warehouse. The message received by the user will allow for the user to fully analyze the links and associations made through the 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 LInX 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 preapproved users. The approval process is role based and must be approved by the agency head to obtain this level of access.

There will be no classified information contained in the LInX data warehouse, it will contain only "law-enforcement sensitive" data. All approved users will have access to the data warehouse dependent upon the role assigned to them by their agency Executive.

It will be the responsibility of the requesting officer or agency, once having accessed the data warehouse, to contact the originating agency that entered the information and obtain permission from that agency to utilize that data in its entirety for any activity that could result in court testimony.

2.4 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:

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

User's rights, also called user privileges, will determine what tasks a user can perform on LInX. User rights can also be established for system administrators at both the system and agency levels to ensure that administrator authority is appropriately restricted and does not exceed an agency's jurisdiction.

The personnel with administrative level access should not have general access to the Security, Tactical or Advanced Analytical screens. Tactical and Analytical users shall not have access to the administrative functions or screens.

2.5 SECURITY ACCESS

Security access provides an authorized individual access to the LInX System 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 LInX System 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 the use of the system.

Security and audit logs will describe what type of action has occurred within the system, which user and user system or agency was involved, the date and time of the action, and the level of the query to include the results. The log identifies the kind of action that was taken, but does not store the actual results of the action. The types of actions that generate audit records include failed login, login, logout, added comment, updated comment, deleted comment, added user, updated user, deleted user, and general query.

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 shall not be held by the same person for any agency.

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

2.6 POSITIVE AND NEGATIVE QUERY RESPONSES

Negative Response to an Inquiry
A negative response is transmitted when no law enforcement record match is found in the LInX System. A negative response to an inquiry may contain a header, the identification of the inquiring agency followed by a notification of no information available or a blank field within each searchable identifier inquired upon.

A negative response should not be used as the sole basis for decision-making by the receiving entity.

Positive Response to an Inquiry
A positive response is transmitted when a law enforcement record(s) is found in the LInX System data warehouse. A positive response contains identifying information by levels of probability for persons, vehicles, addresses and events, the involvement of the inquired subject, and the agency document identification number. In an investigative/analytical inquiry, the recipient will have the ability to utilize all of the retrieved information to conduct prescribed analysis.

As with a negative response, a positive response should not be used as the sole basis for decision-making by the receiving entity.

The results of a positive inquiry should never be utilized as the basis for any court authorized action such as a search warrant, arrest warrant, detention, property seizure, court authorized electronic surveillance, etc. In all instances where further action is to take place based on any level of information obtained as a result of inquiries made to the LInX, that information must be confirmed, verified and validated with the originating agency(s) of the information entered into the data warehouse. Only original documents from the originating agency may be used to support any legal action(s) based on inquires through LInX. LInX screens may not be copied or reproduced in any fashion for use as the basis for any action that could result in court testimony, other than as specified herein with respect to the use of arrest and booking photographs.

2.7 INFORMATION ENTRY

For the LInX data warehouse, the mode of information entry is accomplished through access to the originating agency's records management system data, information or other records source. Each of the participating agencies of the LInX System will normally utilize either an encrypted direct data transport link between the agency's record management system and the data warehouse or the physical front porch (data-mart). Agencies may also utilize other means of transporting data to the data warehouse 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 data warehouse on a regular scheduled or real-time basis.

In the front porch mode, an electronic data transfer will occur on an acceptable schedule to the originating agency, from the originating agency's records management system to the front porch then to the LInX data warehouse. 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 LInX data warehouse.

2.8 INFORMATION MODIFICATION

The purpose of a modification message is to add, delete, or change a portion of data that is part of a record. A record may be add, delete, or change **ONLY** by the originating agency that entered the original record at any time. Even though modification may only be initiated by the originating agency, the need for modification may be brought to the attention of the originating agency by any LInX participant through the use of a modification message. All LInX System users are highly encouraged to notify any participating agency of any information found in the LInX System to be incorrect or erroneous to allow that agency to correct or delete the information from their system and LInX.

2.9 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 originated the record. However, approved agency data integrity staff may request cancellation of a record in the LInX data warehouse 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 or expunged by a judicial order.

2.10 ERROR MESSAGES

A project approved and established error message advises of an error in the LInX System for all data warehouse transactions.

2.11 ADMINISTRATIVE MESSAGES

Administrative messages are utilized to advise users of the LInX System status.

A. An administrative message is transmitted in the format approved and accepted by the sponsoring agency, or designated technical advisory group. Prescheduled maintenance or scheduled outages will be posted on the opening page immediately after sign-in.

B. A message will be transmitted when the LInX System is determined to be out of service. The date and time the system is going out of service is provided as applicable, and the reason, e.g., Out Of Service Today For File Maintenance, etc.
C. A message will be transmitted when a defective transmission (caused by line noise, imperfect transmission of message by the control terminal equipment, time out, etc.) is received at the LInX data warehouse.

All administrative messages will be received upon sign-in by all participating agency terminals regardless of the level of participation in the LInX System.

SECTION 3: QUALITY CONTROL, VALIDATION, AND OTHER PROCEDURES

3.1 MAINTAINING NETWORK INTEGRITY

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the originating agency. However, an approved Administrative Working Group (AWG) can assume a degree of administrative oversight of the data warehouse should the NC LInX Governance Board decide to adopt the practice. Accordingly, the AWG (or other approved entity), would institute appropriate and reasonable quality assurance procedures for all of the users. In relation to Title 42, United States Code 3771, there is a standard that is prescribed for investigative records management and, upon approval of, and with the concurrence of the NC LInX Governance Board and each participating agency; the establishment of maintenance standards for these records could follow these accepted standards. Criminal justice agencies specifically have a duty to maintain records that are accurate, complete, and up-to-date. To ensure reasonably sufficient record management, the AWG would ensure that there are clearly communicated security standards, audit standards, personnel training standards and allow accurate and up-to-date records and proper/secure dissemination of same. Standards will be established by the NC LInX Governance Board with regard to security, audit, and training.

Security:

Security standards are documented in the LInX System Security Authorization Agreement (SSAA) and the NC LInX System Security Policy (SSP). The SSAA documents personnel, physical and technical security, user authorization and authentication, as well as information on dissemination and utilization, while the SSP documents the system policies, processes, etc.

Audit:

The AWG can establish an audit procedure for users, and agencies to ensure compliance with the LInX SSP and other established regulations. In addition to audits conducted, the LInX System shall be independently audited at least once every two years (or other acceptable period designated by the sponsoring agency in conjunction with the NC LInX Governance Board), 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, if required, each user will respond to a preaudit questionnaire which will serve as the audit guideline. A compliance audit by individuals, agencies or the entire system may be conducted on a more frequent basis should it be necessary due to failure to meet standards of compliance or suspicion of misuse.

Compliance audits shall at least cover the following areas:

A. **Accuracy:** Any 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 laws and policies. They should also ensure that audit documentation is available from all users accessing the LInX.

B. **Completeness:** Information contained in an entry from a law enforcement record to be disseminated into the system will contain all of the available associated 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 participating organizations will comply with the SSAA, and the SSP adopted by the NC LInX Governance Board. 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. The security for sensitive information includes eliminating that information from exposure to the LInX System.

E. **Dissemination:** All information will be released in accordance with applicable laws, regulations, and policies established by the NC LInX Governance Board. 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 AWG could ensure that documentation based on the scheduled security audits is available to assist in biennial audits.

Training:

The AWG or their designees, in conjunction with other approved entities can:

A. Train, and affirm the proficiency of system (equipment) operators in order to assure compliance with SSP and other accepted policies and regulations;

B. Biennially, reaffirm the proficiency of system (equipment) operators in order to assure compliance with SSAA and SSP;

C. Maintain records of all training;

D. Initially provide all law enforcement personnel with basic training to ensure effective use of the System and compliance with the SSP and other accepted policies and regulations;

E. Make available appropriate training 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 using methods such as roll call and in-service training;

G. Provide peer-level training on System 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.

3.2 MAINTAINING THE INTEGRITY OF LInX RECORDS

Agencies that participate in and contribute records to the LInX System are responsible for their accuracy, timeliness, and completeness. The integrity of the data warehouse will be maintained through: 1) automatic normalization upon retrieval to NCIC standards; 2) automatic refresh of data which will provide for expungement and 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.

Accuracy:

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

Timeliness:

Records must be contributed promptly to ensure maximum system effectiveness. Prompt availability is defined as regular updating of the data exposed to the LInX System by participating agencies of all law enforcement data, as established and defined by the NC LInX Governance Board.

1. **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.
2. **Timely contribution** of a modification occurs as soon as reasonably possible once the record in question has been retrieved from the originating agency.
3. **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 the system as a result of any other action.

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 or other appropriate databases) 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.

3.3 QUALITY CONTROL

The AWG (or other approved entity), and agency personnel can periodically check records contributed for accuracy. ***All*** errors discovered by or reported to the AWG in the records are classified as serious errors. This classification determines that immediate action must be taken by the originating agency.

Procedures for Errors

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 LInX System are kept accurate, complete, and up-to-date. Upon notification of serious errors, the originating agency will correct the record and the LInX System will retrieve any modified records reflecting accurate information to be included in the data warehouse.

Assumption of a limited responsibility for the cancellation of participating agencies' entries, in connection with the foregoing quality control procedures, does not make the sponsoring agency, NC LInX Governance Board or its designated representatives the guarantor of the accuracy of LInX System records. The originating agency retains complete responsibility for the accuracy, completeness, and current status of its law enforcement records contributed to the LInX System.

3.4 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 LInX System 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 LInX System.

The originating agency will receive requests for records to be validated and will in turn provide validation to the approved LInX user as appropriate in a timely manner, as established by the NC LInX Governance Board, with the full concurrence of each participating agency. Validation procedures will be formalized by the NC LInX Governance Board, with the full concurrence of each participating agency, and copies of these procedures must be on file for review during any audit. In addition, documentation and validation efforts must be maintained for review during such audit.

Validation certification means that:

A. The records obtained through the query have been reviewed and validated by the originating agencies;
B. The records which are no longer current have been removed from the LInX System and all records remaining in the system are valid and active;
C. Records contain all available information; and
D. The information contained in each of the records is accurate.

3.5 RETENTION OF LInX SEARCH RESULTS

A. When an operational inquiry on an individual, vehicle, address, phone number or event yields a valid positive response, any information retained or produced printout showing the inquiry and the record(s) on file in LInX may not be utilized in any fashion or 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 copied from LInX in any manner or placed in an agency's records will be marked accordingly as indicated below and maintained as a permanent part of those records, subject to the authorization and approval of the originating agency.

B. If for any reason of exigency a LInX inquiry yields positive investigative information that must be printed or reproduced in any manner (as a matter of national security or immediate thereat to life), or maintained as an official record within an agency, the employee or analyst (if different from the requesting law enforcement officer, i.e. radio dispatcher, records clerk, etc.), making the inquiry should note directly on the terminal-produced copies precisely:

1. how the information was obtained;
2. when the information was obtained (date/time stamp recommended);
3. who the information was produced for/provided to;
4. initial and date all documents;
5. forward the documentation to the appropriate officer or agency which should be retained in the inquiring agency's investigative case file.

C. If for any reason of exigency photographs are printed from the LInX System for use in suspect identification, witness elimination or an emergency line-up, those photographs must be marked as above and handled in a manner consistent with the rules of evidence. Notification of the originating agency of the use of the photograph will be made within a reasonable period after the use of the photograph, (please refer to Section 1.2.1 herein for further guidance).

3.6 TERMINAL AND/OR LINE FAILURE

A. Every effort will be made to notify users when the LInX System server is going out of service. Each participating agency is also in turn responsible for notification of member agencies when servers connected to the LInX System will be out of service. However, when the LInX server goes out of service unexpectedly, an out-of-service message will be provided for that server. Operational failure of a user's terminal may result from one of four conditions:

1. The LInX Server is out of service;
2. The control server fails or is out of service;
3. A circuit/network problem; or

4. The user's work station malfunctions.

B. When there is system line difficulty or malfunctioning of a data set, the area office of the vendor providing communication service will be immediately notified. It is not always possible to make a specific diagnosis of the trouble. In some cases, it is only known that an agency is not responding or is not responding properly to the LInX server query. If, after a reasonable amount of time, the user's problem has not been rectified, the agency will be requested to contact the vendor or maintenance provider and affect the appropriate adjustments.

C. When an out-of-service status is indicated procedures as established in the formalized system maintenance procedures will be followed. All help desk notifications and technical support will be managed through the level 1 maintenance help desk by the agency approved System Administrator.

3.7 FILE REORGANIZATION AND PURGE SCHEDULE

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

3.8 RESTRICTED SERVICE

Users are advised of restricted service periods will be advertised through the sign-on user screen administrative messages. When the system goes out of service for more than 15 minutes without having previously sent an out-of-service message, a regional notification will be made to advise users of the outage. A "hot-line" telephone number will be available for contact in order to determine/resolve connectivity issues.

3.9 LINX NUMBERS

Each law enforcement record entry message that is accepted for storage in the LInX System data warehouse is assigned a unique LInX number for record identification purposes. The number consists of numeric characters that identify the originating agency for the document. The numbers are not assigned sequentially. The only effect this has on the users is that they cannot expect to find agency law enforcement data within the LInX System entered in sequentially increasing values.

3.10 FEATURES

The unique capabilities of the LInX data warehouse are delineated in multiple documents reflecting the system functionalities and features and will not be repeated herein.

SECTION 4: RESPONSIBILITIES FOR AGENCY CONTROL

4.1 RESPONSIBILITIES

The technical development of the North Carolina LInX System is managed by NCIS as the sponsoring agency in cooperation and with advice, counsel and guidance from the participating federal, state, county and municipal law enforcement partner agencies that constitute the North Carolina LInX Governance Board. The operation, concept and design of the LInX System is managed and controlled by the sponsoring agency in full partnership with the NC LInX Governance Board which provides advice, counsel and guidance on the use, direction and operation of the system. The participating agency executives act as the NC LInX Governance Board providing policy, advice, counsel and guidance on the administrative and operational control and use of the system. The sponsoring agency is responsible for planning and approving necessary hardware, software, funding sources, and training for access to all aspects and levels of the LInX System data warehouse by all authorized participating agencies within the region.

The NC LInX Governance Board consist of the executive managers of all of the participating agencies contributing law enforcement information and data to the LInX System within the region, which includes all federal, state, county and municipal participants. Agency executives who provide advice and guidance as the NC LInX Governance Board, all exercise equal rights and input over the management and direction of the LInX System in full partnership with NCIS. For the purposes of agreements between agencies each Chief, Sheriff, Special Agent in Charge, Director, or Public Safety Director as the head of an agency participating in and contributing to the LInX System will have equal input regardless of the jurisdiction or size of the department. In all instances, agreements obtained through briefings, discussions and presentations will be made by a vote with a simple majority carrying the vote. In all instances agency representation regardless of jurisdiction and affiliation will be limited to one voting participant per agency, with each vote being equal to that of the other participants, regardless of the size and jurisdiction of the agency.

The participating agency executives shall meet as the NC LInX Governance Board to address policies, issues, concerns, modifications, upgrades or any business directly related to the LInX System. Decisions made in this fashion will be binding to all participants who have previously agreed to contribute law enforcement information into the LInX System.

The participating agencies have established a Memorandum of Understanding (MOU) with the sponsoring agency that each agency executive has signed, committing that agency to participation in LInX and participation on an equal basis in partnership with the sponsoring agency. Each agency will agree that decisions made in the above described manner, with regard to the LInX System within the region, will be binding to that agency only with regard to their participation in the LInX System. In all cases, each agency retains ownership of all data exposed within the LInX System and stored within any data warehouse supported by the system.

The NC LInX Governance Board has the right to admit or remove any agency within the region for participation in, or having access to the LInX data warehouse.

Admission or removal of any participating agency will require a unanimous decision by the participants through the governance process.

4.2 COMMITTEES and WORKING GROUPS

General description:

The NC LInX Governance Board may utilize multiple levels of committees and working groups to conduct the business of running the program within the region. Several standard committees may be operated as a matter of routine by the NC LInX Governance Board, while others may be formed for specific tasks then disbanded at the conclusion of that task. Standing committees established should include at least, an Executive Committee and an Oversight Committee. Working Groups should at least include the Administrative Working Group as well as Legal, Technical and User Working Groups.

Executive Committee:

The Executive Committee (EC) should be formed from executive members of the "active" participating agencies in the program. The EC may meet on behalf of the full Governance Board and address the day-to-day dealings with connectivity, expansion, inter-agency issues, or any other matters that require immediate executive level attention to resolve. The EC will have the authority to address anything relating to the LInX System that does not require the attention of the full NC LInX Governance Board as a body, such as matters directly impacting system wide performance, operational procedures, LInX wide general policy formulation, system resources, budget, or overall operational capacity.

Oversight Committee:

Refer to Section 5.1 herein

Other Working Groups:

The NC LInX Governance Board will be encouraged to form specialized working groups (such as the AWG as discussed in Section 3, herein), to address specialized issues or conduct specialized evaluations or provide feedback on specific LInX issues or functions. The working groups may be formed at the discretion of the NC LInX Governance Board and will consist of personnel from the participating agencies with expertise in the areas of interest. The working groups will report either to the EC or directly to the NC LInX Governance Board, at the discretion of the Board.

Recommended permanent working groups include Legal, Technical and User groups should meet regularly and should be actively engaged in all aspects of the program. The evaluations produced by these groups are for the benefit of the sponsoring and participating

agencies to assist in decisions and program direction, and shall not be disseminated outside of the LInX Program.

4.3 DATA ENTRY/UPDATES BY PARTICIPATING AGENCIES

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

B. The NC LInX Governance Board shall be responsible for assuring that every agency that has access by MOU or other interagency agreement will contribute all legally sharable investigative records to the System.

C. Every agency that contributes records must assure that information confirmation is available for all records, within a 24 hour period (or next business day) from the time of inquiry.

D. Every participating agency is responsible for the removal of an investigative record as soon as that agency is aware that the record is no longer valid. It is the responsibility of the LInX data warehouse process to update the data warehouse records by an automated or other retrieval mechanism via the System and in compliance with each partner agency technical capabilities and resources.

4.4 EQUIPMENT AND TECHNOLOGY COMPATIBILITY

Equipment and/or technological incompatibility shall not be sufficient justification, or acceptable for any agency to operate outside of the normal and approved LInX System standards for configuration when participating in the LInX program.

4.5 SERVICES AVAILABILITY

Those services provided by the LInX System to the participating agencies shall be provided to their approved users as prescribed by the sponsoring agency with the exception of:

A. Services specifically limited to System Administrators;
B. Services specifically limited to Security Administrators;
C. 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;
D. Services that may be contrary to a state law, judicial or executive order.

“Users” include those law enforcement agencies approved by the NC LInX Governance Board, as data contributors to the LInX System, and accessing data from the LInX System through any regional dispatch center, regional network, specific agency connection, electronic switch, wireless capability, or other approved computer interface.

The use of any LInX services by any approved agency shall be in accordance with the instructions and procedures established by the MOU, this document, SSP and/or any regulations established and approved by the NC LInX Governance Board.

SECTION 5: LINX OVERSIGHT AND SANCTIONS

5.1 THE LINX OVERSIGHT COMMITTEE

The North Carolina LInX Program shall maintain an Oversight Committee (OC) to monitor and otherwise be aware of and to be the primary contact for the NC LInX Governance Board on the reporting of potential and/or actual violations or allegations of violations of improper or otherwise unwarranted access to, use and dissemination of any information maintained by LInX in the data warehouse.

The OC shall consist of at least three executive management level members of the active LInX participating agencies.

Responsibilities:

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

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

A. The OC will conduct a review of any reported incident of alleged misuse or abuse of access to the electronic data warehouse or of information obtained through the electronic data warehouse by an employee of any user agency.

B. A determination will be made by the OC whether the allegations are administrative or criminal in nature.

C. Once issues are identified, the OC 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.

D. Criminal allegations of illegal access to the electronic data warehouse or illegal use of information obtained from the electronic data warehouse 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:

A. The employing user agency of the accused employee will initiate its own internal investigation within the agency. The employing agency will notify the NC LInX Governance Board through the OC of the nature of the allegation and if the allegation is criminal or administrative in nature.

B. At the conclusion of any investigation conducted by the user agency the results of any investigation will be made known to the NC LInX Governance Board through

the OC. 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 OC or any other participating member by any LInX partner agency, the referral would be made to both the user agency in question and the OC by the partner agency.

A. A recommendation will be made by the OC that the affected agency conduct an internal investigation.

B. The Executive of the affected department shall provide the OC and the NC LInX Governance Board with information of the complaint and with an estimate as to when the investigation will be complete.

The OC is not an investigative body and does not/will not be responsible to conduct investigations.

Responsibilities of the OC are limited to the review of all reported incidents. The OC is charged with:

1) being aware of any misuse of the data warehouse or misuse of information obtained through access to the warehouse;
2) receiving allegations of improper access to the electronic warehouse or misuse of information obtained from the warehouse;
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 Executive Committee (EC) or the NC LInX Governance Board. All incidents that affect the integrity of the LInX System are reported directly to the NC LInX Governance Board.

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

The responsibility of the NC LInX Governance Board is to consider the facts as presented by the OC, the Executive Committee and possibly the Agency affected by the incident. The NC LInX Governance Board will consider only those facts as they specifically pertain to the functional integrity of the LInX information sharing system. As a result of the deliberation of the NC LInX Governance Board, a decision will be made binding on all parties involved. Sanctions recommended must be approved by a unanimous vote of the participating agency executive managers (less the affected agency).

Any sanctions must be:

A. In compliance with the current Memorandum of Understanding;
B. In compliance with the sanctioned and agreed upon Rules;
C. In full compliance with all applicable laws and ordinances.

Sanctions will also be:

A. Imposed for corrective action only;
B. Designed to protect the LInX System;
C. Demonstrate "due diligence" on the part of the NC LInX Governance Board in managing LInX;
D. Specific in nature, and focused only on the related issue;
E. Have a compliance component;
F. Be issued with a precedent in mind.

5.2 LINX OVERSIGHT PROCEDURES

Reporting Allegations:

Minor issues of negligence that are reported either to the agency or directly to the OC, will be reviewed by the OC 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 OC, a corrective recommendation may be included in the review prepared by the OC.

Reportable allegations – any suspected or confirmed improper access to the data warehouse or improper use of information obtained from the data warehouse may be reported to the LInX OC, EC or NC LInX Governance Board in writing, in person or via standard electronic means.

Any allegation that any member of the LInX OC, EC or NC LInX Governance Board becomes aware of will be recorded. The LInX OC will maintain the information and a copy will be shared with the accused employees employing agency.

As a result of any referred report, user agencies will conduct at least a preliminary administrative inquiry or investigation into any LInX related incident. Only 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 OC. Criminal allegations of misconduct will be referred to the appropriate prosecutor with jurisdiction.

All incident investigative findings resulting from information given to the accused employee's agency by the LInX OC, EC or NC LInX Governance Board shall be reviewed by the OC. 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 OC and the user agency investigators consist of a verbal briefing.

A synopsis of the actions taken by the user agency will be presented to OC and will be based on a review of the investigation conducted by the user agency, with a resulting

recommendation for action made by the OC to the NC LInX Governance Board. The recommendation will be reviewed by the EC prior to being presented to the NC LInX Governance Board and the executive managers of the participating agencies, with the EC providing concurrence with the recommendations.

If the EC does not concur with the recommended actions, their position will be presented to the NC LInX Governance Board. The report will include actions recommended by the OC and the EC. Any actions recommended by the OC will be limited to those sanctions approved and adopted by the sponsoring agencies with the full NC LInX Governance Board and made part of the approved LInX Rules of Operation.

If the NC LInX Governance Board determines the user agency did not handle the investigation or any resultant disciplinary action in a manner that maintains the integrity of the System and good faith of the ongoing agreements, the NC LInX Governance Board may take action and impose sanctions on the user agency. Such actions by the NC LInX Governance Board will require a unanimous concurrence of all member agencies (less the affected agency). Any actions will be limited to those provided in the Rules, MOU or the SSP.

Any documents produced as a result of the inquiry or investigation will be made a part of the NC LInX Governance Board's official records and maintained in a secure location. Consideration for the location for storage of 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 approval the facility can be adopted as the permanent storage facility for all records related to the LInX Project.

Sanctions to be considered by the OC for any action related to an incident involving the LInX System are only those designated in the Sanctions portion of the Rules of Operation. At the discretion of the NC LInX Governance Board, 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 LInX System, or with information contained within the LInX System, should immediately have system privileges suspended until conclusion of any level of 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 should have all access suspended until the issue is resolved by the NC LInX Governance Board as a body with that agency.

Addressing allegations of misconduct:

If internal misconduct of an employee is discovered by a member agency it is *recommended* that:

A. The agency head will report any allegations of LInX System misconduct, misuse or negligence by an employee or the agency to the NC LInX Governance Board or the Oversight 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. No investigations of allegations against the agency will be conducted by the NC LInX Governance Board, the sponsoring agency or it's official representative;

D. Investigations will be considered an administrative complaint matter and will be conducted in the same manner (i.e., according to agency policy), as any 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.

1. The agency head, or his representative, will brief the locality's Prosecuting Attorney's Office (PA) on the alleged criminal behavior, and if a prosecutive decision is made that the PA would prosecute if the allegations rise to the level of "probable cause" of criminal conduct, the agency head will turn the investigation over to the appropriate departmental criminal investigators;

2. 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.

   Criminal investigations normally target violations of criminal law while administrative investigations target administrative policy/rules 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.

F. Upon completion of the investigation, the internal investigating body's Commander will produce a report for the agency head;

G. If necessary, the agency head will take appropriate action being consistent with agency and locality rules, procedures, laws and customs as well as compliance with state or federal laws;

H. The agency head will advise the OC that the investigation has been completed;

I. The agency head or appropriate personnel will brief members of the Oversight Committee as to the circumstances, investigation and any actions taken, according to what is permitted by law, agency policies and locality ordinances, rules or regulations.

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

J. The OC will submit a written report to the NC LInX Governance Board and the Sponsoring agency along with a verbal briefing of the allegations, investigative activities and actions taken by the agency head;

K. The NC LInX Governance Board will vote to accept the decision of the agency head in the matter, or reject the decision and, if necessary, impose sanctions on the individual or agency, or call for additional information before deciding;

L. The matter will be made a part of the official records of the NC LInX Governance Board.

If misconduct is discovered by a member agency or reported to the NC LInX Governance Board:

A. If LInX System misconduct, misuse or negligence is alleged to have been committed by an employee of a member agency, the NC LInX Governance Board representative will contact the accused agency head to follow the procedures outlined herein for internal investigations;

B. If LInX System misconduct, misuse or negligence is alleged to have been committed by an agency in general, or an individual directly employed (i.e. a vendor or another individual not directly employed by a participating agency), the OC will be responsible for delegating the investigation to the appropriate investigative body;

C. In the case of 2, (above), the NC LInX Governance Board or the Executive Committee will convene the OC to review all available information prior to the start of the investigation for full concurrence;

D. When the OC requests an investigation, it will be the responsibility of the OC with the concurrence of the NC LInX Governance Board to appropriately monitor that investigative matter;

E. The investigating agency (Internal Affairs or Professional Standards) Commander will directly oversee or conduct the investigation;

1. If criminal conduct is discovered the investigation will cease and the investigating commander will report same to the agency head and the OC;
2. The OC will immediately contact the NC LInX Governance Board, notifying them of the appearance of criminal conduct;

3. The NC LInX Governance Board and the participating agency heads will then convene and a decision will be made on how to further proceed;
4. At a minimum, the NC LInX Governance Board will recommend contact with the prosecuting Attorney's Office in the jurisdiction in which the alleged criminal conduct was thought to have occurred. The investigators will brief the Prosecuting Attorney, as well as receive a prosecutive decision if the allegations rise to the level of "probable cause" of criminal conduct;
5. If the locality's Prosecuting Attorney makes a decision to prosecute, the affected agency will turn the investigation over to the agency's internal or criminal investigators;
6. In all cases of allegations of criminal conduct by an agency, the NC LInX Governance Board will turn the matter over to the appropriate investigative jurisdiction.

F. 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;

G. The investigating body's commander will complete a report at the conclusion of the investigation and present it to the OC;

1. Any report or documentation prepared and submitted will be in compliance with all privacy, legal, policy and disclosure requirements.

H. The OC may decide to take the committee recommendation to the NC LInX Governance Board or ask for additional investigation or clarification;

I. The OC will present the findings to the NC LInX Governance Board and the executives of the participating agencies with recommendations for appropriate sanctions;

J. If the allegations are determined to be substantiated either as criminal or administrative issues with respect to the LInX System, the NC LInX Governance Board could impose administrative sanctions, as it deems appropriate.

K. Administrative sanctions must be approved by a unanimous vote of the NC LInX Governance Board (less the affected Agency).

5.3 INTRODUCTION TO LINX SANCTIONS

A. Purging of an agency's investigative records and discontinuance of LInX System access for an agency are the two ultimate sanctions available to the NC LInX Governance Board for enforcement of LInX System policies and procedures. 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.

B. Considerations:

1. An up-to-date MOU and approved Rules of Operations and SSP should be in place with the NC LInX Governance Board, the Sponsoring agency 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, SSP or any criminal breaches.

2. 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. Unauthorized disclosure (non-criminal)
ix. Criminal misconduct

C. A special audit of a participating agency with access will be part of the sanction package upon request of the sponsoring agency or the NC LInX Governance Board.

D. In matters involving an agency participating in a substandard manner flagging that agency's records will be an option of the NC LInX Governance Board.

E. Deadlines will be imposed on compliance with corrective action notices.

5.4 SANCTIONS

Specific sanctions for administrative matters are recommended to include:

A. A message transmitted by the Oversight Committee on behalf of the NC LInX Governance Board in writing to the participating agency for all noted issues and/or errors. The NC LInX Governance Board administrative representative is to maintain copy of these messages for follow-up, and as a matter of record for a period not to exceed one year from the date corrective action has been verified by the Oversight Committee and approved by the NC LInX Governance Board.

In matters where agencies have been notified of repeated substandard practices over consecutive years, all of the related records will be kept for a period not exceeding one year from the date corrective action has been verified by the Oversight Committee and approved by the NC LInX Governance Board.

B. A letter of request for compliance regarding:

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);
7. Serious failure of a participating agency to ensure compliance with confirmation and validation policy.

C. Letter of intent to remove the participating agency from the system if deficiencies are not corrected including:

1. Continuous error trends;
2. Audit failure status (not corrected within recommended time-frames of first request);
3. Unauthorized disclosure of investigative information (non-criminal);
4. Intentional (criminal) disclosure or misuse of investigative information;
5. Continuous failure to ensure compliance with confirmation and validation policy.

D. Removal from the system includes the removal of access to all agency records and discontinuance of service pending reinstatement approval by the NC LInX Governance Board.

E. Reinstatement:

1. Upon satisfactory proof that the offending participating agency has corrected its deficiencies, with verification of the Oversight Committee, the NC LInX Governance Board may reinstate.

Specific sanctions directed for administrative infractions or criminal acts are recommended to include:

A. In non-criminal matters, a letter may be transmitted by the Oversight Committee on behalf of the NC LInX Governance Board in writing to the participating agency. The NC LInX Governance Board administrative representative is to maintain copy of these messages for follow-up, and as a matter of record for a period not to exceed one year from the date corrective action has been verified by the Oversight Committee and approved by the NC LInX Governance Board.

In non-criminal matters where personnel have been notified of repeated improper actions over consecutive years, all of the related records will be kept for a period not exceeding one year from the date corrective action has been verified by the Oversight Committee and approved by the NC LInX Governance Board.

B. In all matters where an administrative personnel issue has been brought to the attention of the Oversight Committee or the NC LInX Governance Board, with regard to any user of the system, sanctions could be recommended or imposed by the NC LInX Governance Board. In all instances the NC LInX Governance Board reserves the right to impose or waive sanctions at their discretion in the following manner:

1. Verbal request to the user's agency for counseling on compliance;
2. Written request to the user's agency for counseling on compliance;
3. Written recommendation for retraining;
4. Written notification for repeated non-compliance with a recommendation for internal performance based action;
5. Suspension of user privileges for a period agreed upon as appropriate by the NC LInX Governance Board;
6. Permanent revocation of user privileges as agreed upon by the NC LInX Governance Board.

C. In all matters where there are allegations of criminal misconduct involving the use of the LInX System, user privileges will be immediately suspended until the matter is resolved to the satisfaction of the user's agency, the NC LInX Governance Board and the sponsoring agency. Any allegations of criminal misconduct will be referred to and addressed by the appropriate investigative agency and/or prosecutor, as indicated herein.

Criminal prosecution of any user for actions related to the use of the LInX System will result in permanent suspension of access to the system by that user.

Recommended procedures for addressing any incident involving LInX users brought to the attention of the Oversight Committee, the sponsoring agency, or NC LInX Governance Board are established in Section 5.2 herein.