

SHARED SERVICES AGREEMENT

County-Wide Criminal Justice Information System Network Agreement Between the County of Essex, NJ and

Preliminary Statement

This Agreement is entered into pursuant to the provisions of the Uniform Shared Services and Consolidation Act (N.J.S.A.40A:65-1 et seq.) among the County of Essex (the "County") and the respective municipalities within the County who are signatory hereto (each a "Municipality")

WHEREAS, the County-Wide Criminal Justice Information System (CJIS) Network, including its related products, services, support and recurring line charges, allows for the connectivity of a municipal police department to the County via a private IP Network, and;

WHEREAS, the routers provided as a part of this Agreement will be configured to encrypt NJSP CJIS transmissions, Integrated Law Enforcement Initiative (ILEI) transmissions and other traffic as identified by the ILEI governing committee, and;

WHEREAS, some, Municipalities will also transmit video traffic (video arraignment) where the routers will be configured for split tunneling and the video traffic will not be encrypted.

NOW THEREFORE, its agreed as follows:

AGREEMENT

1. The County hereby grants the Municipality the right to participate in the County-wide CJIS Network as provided hereunder. The County-wide CJIS Network is defined as the County-wide Private IP Network and associated equipment, NJSP CJIS connectivity, the ILEI Solution and the Fingerprint Store and Forward Solution.
2. The Municipality will pay the County for the right to participate in the CJIS Network:
 - (a) An annual fee of \$15,000 per line on or before March 1, 2012, provided, however, this fee is subject to change depending upon the aggregate number of lines used by all Municipalities. This fee includes:
 - (1) Recurring line charges and managed network services fees paid by the County to Verizon Business Network Services, Inc.;
 - (2) Annual maintenance fees for the ILEI solution paid by the County to Enforsys, Inc.;
 - (3) Annual maintenance fees for the Fingerprint Store and Forward solution paid by the County to Clearview Data Systems, Inc.;
 - (4) Annual maintenance fees for the equipment and system Software;
and,
 - (5) System Administrator support services.

(b) Subsequent annual payments will be on the anniversary of the due date of the first annual payment.

3. The County intends to enter into agreements with vendors for Maintenance and Support Services. In case of any material changes in the maintenance and support agreements, all Municipalities which are current in their payments to the County hereunder, will receive prior and timely notification of such changes. Whenever new major releases of the software are planned, all Municipalities which are current in their payments to the County hereunder, will receive prior and timely notification of the new release.
4. Prior to the general use of the CJIS Network by Municipality, it and the County will mutually agree upon a process for Technical Problem Notification and follow up. A Bug Report of known problems which could potentially impact the Municipality will also be issued periodically with project completion dates for bug fixes, if available. The parties will also put in place a mutually agreed process for (a) User Acceptance Testing for problem fixes; and (b) Notification of planned outages for the system to the Municipality; and (c) Training of Municipal users and availability of appropriate user documentation.

5. The ResponseAbility Records Management Reporting Software is the exclusive property of Enforsys, Inc. ("Enforsys"). Enforsys owns the title, copyright, and other intellectual property rights in the ResponseAbility Records Management Reporting Software which is licensed by Enforsys to the County, and is protected by copyright and other intellectual property laws and treaties. Except for those rights expressly granted by Enforsys, it retains all proprietary rights to the ResponseAbility Records Management Reporting Software. The ResponseAbility Records Management Reporting Software may not be reproduced, exploited, modified, transmitted, licensed or distributed without the prior written consent of Enforsys. No user may disassemble, decompile, or reverse engineer the ResponseAbility Records Management Reporting Software.
6. The Dataworks Plus programs are the exclusive property of DataWorks Plus through Clearview Data Systems. DataWorks Plus owns the title, copyright, and other intellectual property rights in the DataWorks Plus programs which are licensed to the County, and are protected by copyright and other intellectual property laws and treaties. Except for those rights expressly granted by DataWorks Plus through Clearview Data Systems, it retains all proprietary rights to the DataWorks Plus programs. The DataWorks Plus programs may not be reproduced, exploited, modified, transmitted, licensed or distributed without the prior written consent of DataWorks Plus. No user may disassemble, decompile, or reverse engineer the DataWorks Plus programs.

7. This Agreement shall become effective as to any signatory Municipality as of the date of execution hereof by the Municipality and shall terminate, on February 28, 2015, unless terminated prior thereto as provided in paragraph 8 hereof, or extended by mutual agreement of the parties.
8. A Municipality may terminate this Agreement upon ninety (90) days written notice to the County. The County may terminate this Agreement upon thirty (30) days written notice to the Municipality if the Municipality fails to make any payment(s) required under this Agreement or is otherwise in material breach of any provision hereof, and has not remedied such failure or breach within fifteen (15) days after the giving of written notice thereof. In case any of the agreements between County and either Verizon, Enforsys or Clearview Data Systems is terminated, County shall notify the Municipality of such termination immediately and, unless an alternative is contracted for by the County, this Agreement shall thereupon terminate.
9. Nothing provided in this Agreement precludes a Municipality from negotiating directly with Verizon, Enforsys or Clearview Data Systems, independent of this Agreement, for any additional products, services, enhancements or add-ons, so long as any such addition is compatible with, and has no adverse impact upon, the CJIS Network. Any such separate agreement must be negotiated by the Municipality directly with the respective vendor, including all contractual terms and conditions, licensing arrangements and associated costs, all of which are the sole responsibility and obligation of the Municipality.

10. The County makes no warranties, either express or implied as to any program, process, software, equipment or the like utilized hereunder. The County shall not be liable to the Municipality for damages of any kind arising from the County's performance, non-performance or negligent performance hereunder, or resulting from, relating to, or arising out of the use of any program, process, software, equipment or the like hereunder.
11. In order to access the CJIS Network, the Municipality and its authorized users must agree to and execute the terms of the Memorandum of Understanding, including its appendices, a copy of which is attached hereto, as Exhibit "A".
12. This Agreement may not be amended or modified, in whole or in part, except by a writing signed by the parties hereto.

IN WITNESS WHEREOF, the parties have executed this Agreement as of

this _____ day of _____ 201__.

ATTEST:

MUNICIPALITY

By: _____

Name:

Title:

Date:

ATTEST:

ESSEX COUNTY

By: _____

Name:

Title:

Date:

Integrated Law Enforcement Initiative (ILEI)
"Memorandum of Understanding"
For Participating Law Enforcement Agencies

**MEMORANDUM OF AGREEMENT BETWEEN THE COUNTY
OF ESSEX AND THE PARTICIPATING LAW ENFORCEMENT
AGENCIES WITHIN THE COUNTY OF ESSEX TO CREATE
AND PARTICIPATE IN THE ESSEX COUNTY "INTEGRATED
LAW ENFORCEMENT INITIATIVE"**

1. Purpose

This agreement is made between the various participating County and Municipal Law Enforcement agencies to provide access to the *Essex County Integrated Law Enforcement Initiative* (herein after referred to as "ILEI") that will enhance the sharing of law enforcement services and information. "The ILEI System" will also share information with the statewide system known as New Jersey Data Exchange (NJ DEx), which is designed to promote the dissemination and sharing of law enforcement services and information on a statewide basis. In order to participate in, and contribute to the New Jersey Data Exchange (NJ DEx), the participating agency must agree to all of the terms of the MOU Memorandum of Understanding for the Contribution of Data into the New Jersey Data Exchange (NJ-DEx) in place between the New Jersey Department of Law and Public Safety, Division of State Police, Office of Homeland Security and Preparedness and the Essex County Sheriff. (Copy attached as Appendix B).

The activities of the participating agencies shall be conducted in accordance with all applicable federal, state, and local laws and statutes, regulations, and requirements. Additionally, this agreement is subject to periodic modification pursuant to notice to all participating agencies.

Participating agencies shall employ rigorous procedures to assure that the security / privacy of all information is adequately provided for, and that information shall only be used for law enforcement, criminal justice and other lawful purposes.

2. Participants

The parties to this agreement are the County of *Essex* ("County"), the *Essex County Sheriff's Office* ("Sheriff"), the *Essex County Prosecutors Office* ("Prosecutor"), the *Essex County*

Department of Corrections ("Corrections") and each of the participating municipalities as set forth in Appendix A of this agreement, titled "Participating Municipalities". This agreement may be amended at a future date to include the New Jersey State Police as well as other law enforcement agencies from other counties, the State and/or the federal government.

3. Definitions

- A. "CAD/Records Management System" means a computer-aided dispatching and records management system which is used by the participating law enforcement agencies for the dispatching of response units, the capture of key information and the management of records for those agencies.
- B. "Chief of Police" means the duly appointed Chief of Police of a municipal police department located in the County of *Essex*.
- C. "Chief Law Enforcement Executive" means the highest ranking sworn law enforcement officer of any community where there has not been a Chief of Police appointed.
- D. "Committee" means a group of individuals as designated by the Chiefs of Police/Chief Law Enforcement Executives/Directors who meet to discuss issues related to the ILEI System and make recommendations for improvement, as appropriate.
- E. "County" means the County of *Essex*.
- F. "Director" means a civilian director of public safety designated by local ordinance as the appropriate authority to adopt rules and regulations governing the police department.
- G. "ILEI Governing Committee" means the group of individuals who represent the interests of all the stakeholders of the project.
- H. "ILEI" means Integrated Law Enforcement Initiative.
- I. "New Jersey Data Exchange" means a statewide system known as NJ DEx, a database by which law enforcement information is downloaded, stored and can be accessed by/shared with any other participating law enforcement agency.
- J. "OPRA" means the Open Public Records Act.
- K. "Secondary Dissemination" means the release or dissemination of information either in written form or orally, that was learned or obtained through the use of the *Essex County* Integrated Law Enforcement Information Sharing System to unauthorized persons or for an unauthorized purpose.

L. "Systems Manager" means the designee of the County who is responsible for managing the System.

4. Service Agreement

This agreement shall be considered a part of a shared service agreement, referenced as Appendix "A," between and among the participating law enforcement agencies and the County. The establishment of this information sharing initiative does not supplant, change, alter or otherwise modify any pre-existing agreement(s) between or among the parties to this agreement or within the individual law enforcement agencies.

5. Scope of Project

This project shall consist of customized applications based on Internet technology which will enable participating law enforcement agencies to access shared law enforcement data via a secure internet connection, utilizing a logon and password provided to them by the County. This phase of the project will be available to those law enforcement agencies not previously upgraded to access this data.

6. Use of Data/Sharing of Information

The data that is subject to this agreement shall be used to enhance the participating law enforcement agency's ability to deliver law enforcement services to its constituents, to improve the participating agency's ability to investigate crimes or offenses, to make the participating agency more efficient and to improve officer safety. The ILEI System is designed to promote the exchange of information between participating law enforcement agencies, which provides for more effective inter-agency communications. This promotes interoperability and cooperation between agencies that are presently on different computerized records and dispatch systems, as well as the relaying of urgent and timely information. This also enhances the efficiency and safety of participating agencies through real time, field unit-to-unit, and information exchange interoperability. This System is being implemented in phases, which include, creating a hardware "backbone", creating a software "middleware" for exchange with each participating agency, and

adding agencies with CAD/Records Management Systems. The ILEI System can also provide the ability to query the central repository data through mobile devices.

7. Use of ILEI System

A. The ILEI System is intended for use when the exchange of law enforcement information, statistics and messages, will enhance the safety and effectiveness of personnel dealing with an incident, investigating a crime or offense, or when providing a law enforcement service to the community. *The ILEI System is not to be used to deliver personal information or messages or to obtain information which will be used for personal or non-law enforcement purposes.* The ILEI System may be used to allow data exchange or messaging between multi-jurisdictional agency command personnel dealing with an incident.

(1) Only data exchanges that relate to official agency activities are permissible. The expectation of timely entries of all relevant data may include, but not be limited to:

- (a) Reporting occurring or previous agency activity;
- (b) Reporting incident data;
- (c) Reporting arrest data;
- (d) Reporting traffic data, accident and enforcement data;
- (e) Providing master name information.

Entry of the above reports into the ILEI System does not invoke the requirements and obligations as set forth in 28 CFR, Part 23 federal regulations. To the extent that a participating agency selects to submit intelligence as defined by 28 CFR, Part 23, the submitting agency must comply with the most recently updated Attorney General Guidelines. Criminal Intelligence data is frequently composed of uncorroborated allegations or suspicion of criminal activity, and does not always contain information concerning adjudications and final judicial dispositions.

B. Only official messages relating to authorized law enforcement personnel are permitted.

- C. Use of the ILEI System's enhanced features is limited to official and authorized law enforcement personnel and for legitimate law enforcement purposes. Use of these enhanced features for non-law enforcement purposes or for any personal purpose is a violation of this agreement.
- D. The "secondary dissemination" of information obtained from the use of the ILEI System to unauthorized parties is prohibited. This includes both electronic and paper reproduction.
- E. The dissemination of lawfully discoverable materials / information pursuant R. 3:13-3 of the Rules Governing Criminal Practice obtained from the ILEI System shall be permitted pursuant to authorization by the Essex County Prosecutor or any Assistant Prosecutor authorized by the Essex County Prosecutor to provide discovery pursuant the Rules Governing Criminal Practice. Such information may be "redacted" by the Essex County Prosecutor or any Assistant Prosecutor authorized by the Essex County Prosecutor to provide discovery pursuant the Rules Governing Criminal Practice or by the publishing agency where appropriate and for the purpose of protecting sensitive information pursuant to the authority, supervision and discretion of the Essex County Prosecutor or his or her designee.

8. Participation and Submission of Data/Information Responsibilities

Each agency which elects to participate in the ILEI System will maintain ownership of and shall be solely responsible for the content, accuracy, timeliness, and updating of the information that it posts to the ILEI System database. All such information shall remain the property of the posting agency. Each participating agency agrees to permit other authorized users of the ILEI System to view that data, information, and messages for the purpose of furthering the law enforcement mission and goals. By enabling the sharing of law enforcement data across multiple jurisdictions, the County shall provide a valuable service to its constituents by reducing a known criminal's ability to evade police identification and detection. The specific responsibilities and restrictions that are assumed by each participating law enforcement agency are as follows:

- A. The Chief of Police/Chief Law Enforcement Executive/Director of each participating agency shall determine what information and data shall be uploaded and posted to the ILEI System.
- B. Each participating agency shall have the right to remove any and all information and data that it has placed on the ILEI System at any time or for any reason deemed appropriate by the Chief of Police/Chief Law Enforcement Executive/Director provided that the Prosecutor is provided written notification in advance of the removal of said information and the Prosecutor approves the action.
- C. Agencies, or employees of any agency participating in the ILEI System, may not release any information that was posted, uploaded, or entered into the ILEI System by a participating agency or that is otherwise owned by a participating agency, to any unauthorized person, individual, entity, business, group, agency, or organization. Any such unauthorized release shall be considered a "secondary dissemination" and is specifically prohibited by this agreement.
- D. The ILEI System may contain data related to the operation and use of ILEI System resources, authorized users of the ILEI System, and technical data such as tables, libraries, and other items necessary for the operation of the overall System. Personnel supporting the operation of the ILEI System are solely responsible for keeping such information current and up to date.
- E. The ILEI System shall be used for criminal justice purposes only. Any unauthorized or personal use of the ILEI System or of any of the enhanced features of the ILEI System shall constitute a violation of this agreement. The Essex County Prosecutor or his or her designee shall determine what parties shall constitute authorized recipients of information or data contained in the ILEI System and for what purposes such information or data may be used or disseminated.

9. Reports and Secondary Dissemination

- A. The ILEI System shall not maintain any reports or data concerning operational procedures, bulletins, and/or other related information posted or exchanged by the agencies participating in the ILEI System. Only those documents agreed to by the ILEI Governing Committee shall be maintained in the ILEI system. All information contained in the database hosted and maintained by the ILEI System pertaining to the documents submitted by each participating agency shall remain under the direct control of the submitting agency.
- B. Personnel from any consulting or assisting agency or company involved in the maintenance of the ILEI System and equipment have no right to and are specifically prohibited from releasing any information or data placed on the ILEI System by the participating agencies, the County, or by any other authorized person or entity.
- C. Each participating agency is solely responsible for the appropriate release of its own data and information to the ILEI System.
- D. All OPRA requests shall be forwarded to the appropriate participating agency for review and response. In providing responses to the person or entity requesting the record or records, the cause for denial shall be stated, and the person or entity shall be notified that the ILEI System is not the custodian of records for the requested information.

10. System Security

- A. Misuse of information that is maintained in or provided to the ILEI System can have severe repercussions. Carelessness or misuse of such information and the unauthorized release of such information can compromise pending law enforcement cases, violate the privacy rights of citizens, violate the federal and state constitutional rights of citizens, and in severe cases, destroy reputations or jeopardize the security of individuals including witnesses and victims of criminal activity. The intentional misuse of such information can also violate various criminal statutes.

B. The penalties for misuse of the ILEI System and the information contained therein include:

- (1) Sanctions (administrative, criminal, internal, etc.) may be initiated against a participating agency and its personnel for failing to ensure that the agency and its authorized users comply with any segment of this agreement and with the rules contained therein.

Possible sanctions include but are not limited to:

- (a) If the violation of this agreement is determined to be intentional and continuous in nature, termination of all ILEI System services (submission of data, access, etc.);
- (b) Purging of agency records from the ILEI System;
- (c) Criminal Prosecution. Criminal penalties for those individuals who profit or attempt to profit or benefit from or misuse the ILEI System and the information contained therein;
- (d) Administrative disciplinary action against those individuals who misuse the ILEI System and/or violate any of the provisions of this agreement, or those individuals who fail to properly perform their supervisory responsibilities associated with the ILEI System. Such action may involve the imposition of fine, suspension and/or dismissal against the employee by their respective participating agency to the extent permitted by law.
- (e) Civil prosecution.

(2) Examples of violations that may lead to sanctions include but are not limited to:

- (a) Failure to comply with the provisions of this agreement and/or for a violation of the terms and conditions, thereof.
- (b) Failure to follow/adhere to the ILEI System's policies and procedures.
- (c) Failure to follow/adhere to the ILEI's Security Policy (Copy attached as Appendix C).
- (d) Failure to participate in training sessions, and/or meet the training requirements for users and operators of the ILEI System.

N-DEx's proposed services and capabilities, N-DEx will allow participating agencies to detect relationships between people, places, things and crime characteristics; to link information across jurisdictions; and to "connect the dots" between apparently unrelated data without causing information overload. This capability will occur primarily in the realm of structured data but can also include unstructured data. In addition, N-DEx will provide contact information and collaboration tools for law enforcement agencies that are working on cases of mutual interest. Ownership of data shared through N-DEx will remain with the law enforcement agency that provided it.

Indemnification

The User agrees to indemnify and save harmless NJCJIS management, its employees and officials from and against any and all claims, demands, action, suit, and proceedings brought by others, and for negligence or other tortious conduct of the User, including, but not limited to, any liability for any loss, cost, expense, and damages by reason of any claim of false imprisonment, false arrest, or any other case of action, in the exercise and enjoyment of this agreement. This agreement shall be liberally construed to apply to both types of users, those equipped with a NJCJIS terminal and those participating via another agency's terminal. Unless specifically addressed by the terms of this MOU (or other written agreement), the parties agree to only be responsible for the negligent or wrongful acts or omissions of their respective officers and employees, but only to the extent they would be liable under the laws of the jurisdiction(s) to which they are subject.

Acknowledgement

We hereby acknowledge the duties and responsibilities set forth in this MOU and in the documents, subject matter, and procedures incorporated by reference. We acknowledge that these duties and responsibilities have been developed and approved in order to provide information to the NJ-DEx database and ensure that it is maintained with the integrity, and discipline considerations outlined herein. We further acknowledge that failure to comply with these commitments will subject the user agency to various sanctions outlined in the NJCJIS Noncompliance Sanction Plan. These sanctions may include the termination of NJ-DEx and/or NJCJIS services to the User.

This MOU shall become effective when all duly authorized representatives of each party have signed the document and shall.

**CRIMINAL JUSTICE INFORMATION SYSTEM MEMORANDUM OF
UNDERSTANDING NJ-DEX ACKNOWLEDGEMENT**

Signed as dated, the parties hereto caused this agreement to be executed by the proper officers or officials, in witness hereof. Effective date is: _____.

New Jersey Department of Law and Public Safety,
Division of State Police

By: _____

Title: Superintendent of State Police

Date: _____

Office of Homeland Security

By: _____

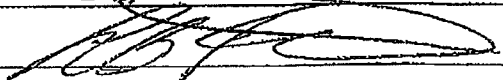
Title: Director

Date: _____

Criminal Justice Agency
Agency Head/Administrator

By: ARMANDO B. FONTOURA (Please Print)

Title: SHERIFF

Signature: 

Agency Name: Essex County Sheriff

Agency Address: 50 W. MARKET ST., NEWARK, NJ 07102

ORI Number : NJ 0070000

Date: 6/26/2009

All questions concerning this agreement should be directed to the NJCJIS Control Unit, State Bureau of Identification, Identification and Information Technology Section, at 609-882-2000, extension 2294.

Appendix C

Essex County Integrated Law Enforcement Initiative Security Policy.

**Essex County
Integrated Law Enforcement Initiative
Security Policy**

Table of Contents

1.0	Introduction	3
1.1	The Essex County Integrated Law Enforcement Initiative	3
2.0	Information Collection	4
2.1	ILEI Overview	4
2.2	Data Source	4
2.3	Data Quality	4
3.0	Security	5
3.1	Access Rules	5
3.2	Periodic Audit	5
3.3	User Eligibility Requirements	6
3.4	ILEI Access Approval	6
3.5	Password Policy	7
4.0	Access Accountability	8
4.1	Roles and Privileges	8
4.2	Accountability	8
4.3	User Responsibility	8
5.0	Addendum: Essex County Integrated Law Enforcement Initiative – User Application Form	9
6.0	Addendum: Essex County Integrated Law Enforcement Initiative- User Access Form	10

1.0 Introduction

1.1 The Essex County Integrated Law Enforcement Initiative

The Essex County Integrated Law Enforcement Initiative, ILEI, is transforming the current County's law enforcement environment of multiple, disparate IT systems and paper documents into an integrated system of electronic information sharing among the ILEI participants. The following agencies makeup the initial (Phase I) membership of the ILEI:

- Essex County Department of Corrections;
- Essex County Prosecutor's Office;
- Essex County Sheriff's Office; and
- City of Newark Police Department.

The Phase II deployment incorporates the remaining twenty-one local municipal Police Departments.

The ILEI Governing Committee consists of individuals representing the interests of all the Stakeholders of the project and meets on a regular basis. This committee currently consists of a representative from:

- Essex County Office of the County Administrator;
- Essex County Department of Corrections;
- Essex County Prosecutor's Office;
- Essex County Sheriff's Office;
- City of Newark Police Department; and
- Essex County Chief's of Police Association.

This Committee is responsible for defining user access and accountability for ILEI participants. This Committee is also responsible for defining and releasing Policy and Procedure Guidelines as the Committee deems necessary for all Law Enforcement and Judicial System Processes that are implemented in the Integrated Platform.

2.0 Information Collection

2.1 ILEI Overview

In order to protect the public and help defend against terrorism, law enforcement must be able to share data in an efficient and secure environment that transcends both jurisdictional and technological boundaries. The ILEI Application allows available information to be easily published and accessed in real time, enabling law enforcement and criminal justice personnel to make decisions based upon accurate and timely information.

2.2 Data Source

A member agency will transmit selected data from their records management system to the ILEI repository. Each agency will make a determination as to what information (from a pre-determined list of available report types) will be contributed to the ILEI Repository. Data from each participating agency will be acquired to refresh the ILEI Database by automated updates on a predetermined schedule.

2.3 Data Quality

The ILEI participants will remain the owners of the data being contributed and will be therefore, responsible, once received, for the content, quality, accuracy, timeliness and updating of the data accessed through ILEI.

3.0 Security

3.1 Access Rules

All personnel having access to the ILEI Repository agree to abide by the following rules:

- ILEI data will be used for legitimate law enforcement related duties as well as judicial processing as authorized by the User's employer.
- Use of the ILEI Repository is limited to those individuals who have been selected, approved and trained.
- Information accessed through the ILEI Repository cannot be:
 1. Sold, published, exchanged or disclosed for commercial purposes; or
 2. Disseminated to unauthorized persons.
- Each individual will be responsible for maintaining the privacy of their own password. Individual passwords will not be disclosed or used by any other person except as authorized.
- Individual passwords will be changed if authorized personnel of the agency or members of the Essex County ILEI Governing Committee suspect the password has been improperly disclosed or otherwise compromised.
- Password reset will be managed centrally by the ILEI System Administrator.
- Use of the ILEI data in an unauthorized or illegal manner will subject the User to denial of further access and possible criminal prosecution as detailed in the Memorandum of Understanding signed between the Participating Agency and the County of Essex.

3.2 Periodic Audit

The Essex County ILEI Governing Committee will be responsible for conducting or coordinating audits and investigating misuse of ILEI source information, ILEI Application or any provision of this Security Policy.

3.3 User Eligibility Requirements

Access to information contained within the ILEI Repository will be granted to full time law enforcement officers based upon the submission of an approved User Application Form. Others, including individuals employed by a law enforcement agency as civilians or technical support staff employed by a non-law enforcement agency that have direct access to ILEI Repository data must also submit to a background investigation. The background investigation will include complete state and federal applicant fingerprint cards submitted to the New Jersey State Police, State Bureau of Identification. The employing agency must check the following state and national arrest and fugitive files:

- New Jersey Computerized Criminal History (NJCCH);
- New Jersey Wanted Person System (NJWPS);
- NCIC Interstate Identification Index (III);
- NCIC Wanted Person File; and
- National Law Enforcement Telecommunication System (NLETS) Criminal History Record Information (CHRI) for non III participant states.

Note: Background Screening Process is based upon NJCJIS Guidelines.

3.4 ILEI Access Approval

The local agency ILEI Liaison Officer will complete the User Application Form; a copy of this Application Form is attached to this Security Policy as an addendum. The User will acknowledge and certify that he / she has read the ILEI Security Policy and agrees to be bound by the policy's provisions.

The local agency ILEI Liaison Officer will certify that the named User meets the eligibility requirements as specified in the ILEI Security Policy. The completed application will be forwarded to the respective agency head for review and endorsement. This completed application for an ILEI User ID will be forwarded in a transmittal letter to the Essex County ILEI System Administrator for submission to the ILEI Governing Committee final approval.

Once approved, the User will sign the User Access Form; a copy of this Access Form is attached to this Security Policy as an addendum. The User will acknowledge and certify that he / she has been trained in the functionality of the ILEI Application.

3.5 Password Policy

When a new User initially signs onto the ILEI Application he / she will be directed to create a new password. The password is case sensitive. The Password Policy will include the following requirements:

- Password must be a minimum of eight characters;
- Password must include at least one capital letter;
- Password must include at least one number;
- Password must include at least one special character;
- Password must be changed every sixty days and the new password cannot be the same as any of the previous five passwords; and
- The system will lock out a user from signing onto the system if an incorrect password is entered seven consecutive times.

A user who has been locked out of the system due to exceeding the number of consecutive password login attempts must receive a new password from the ILEI System Administrator.

4.0 Access Accountability

4.1 Roles and Privileges

Every User of the ILEI Application will have a unique login ID and password. Every User will belong to a group based upon the agency, job title and description.

4.2 Accountability

When a request for information is transmitted from a User to the ILEI Repository, the request is automatically logged by the system identifying the User viewing the resulting information. When such information is disseminated outside of the agency from which the original request is made, a secondary dissemination log must be maintained by the originating agency in order to correct possible erroneous information as well as for auditing purposes. Secondary dissemination of information can only be to a law enforcement agency for a law enforcement purpose. A record of such dissemination must be maintained by the respective agency separately from ILEI and will record, as a minimum, the following information:

- Date of Release;
- To whom the information relates, subject, SBI and or FBI numbers that clearly identifies the information released;
- To whom the information was released to including Agency, Address and Telephone Number; and
- The purpose for which the information was requested.

4.3 User Responsibility

Individual Users remain responsible for the information and its appropriate use, as well as the shredding of records that were copied from the ILEI Repository but are no longer needed. Failure to abide by the provisions of this Security Policy may result in the suspension or termination of access privileges, discipline sanctions imposed by the User's employing agency and/or criminal prosecution as detailed in the Memorandum of Understanding signed between the Participating Agency and the County of Essex.

5.0 Addendum: Essex County Integrated Law Enforcement Initiative – User Application Form

ILEI User Application Form

ILEI User ID Request

Agency Name:

User:

First Name

Middle Initial

Last Name

E-mail Address:

Job Title/Description:

(Ex. Assistant Prosecutor, Police Officer, Investigator, CJP, Corrections)

Qualification:

User acceptance and level of access are based upon the Security Policy created by the Essex County ILEI Governing Committee. The Agency ILEI Liaison Officer certifies that the above mentioned User meets the qualifications described in the ILEI Security Policy, based upon personal review of the following:

- ☐ The User is a Full-time Law Enforcement Officer in good standing
- ☐ As a civilian police employee who has satisfied the ILEI Security Policy requirements based upon a review of a state and national criminal history check based on fingerprint identification

User Certification:

I, _____, [Name of Agency] ILEI User, acknowledge and certify that I have read the ILEI Security Policy and agree to be bound by their provisions.

Signature

Date

Agency ILEI Administrator Certification:

I, _____, ILEI Liaison Officer for the above mentioned agency verify the above named User meets the ILEI eligibility as specified in the Security Policy established by the Essex County ILEI Governing Committee.

Signature

Date

6.0 Addendum: Essex County Integrated Law Enforcement Initiative- User Access Form

User Access Form

ILEI User ID Request

Agency Name:

User:

First Name

Middle Initial

Last Name

E-mail Address:

Job Title/Description:

(Ex. Assistant Prosecutor, Police Officer, Investigator, CJP, Corrections)

Qualification:

User acceptance and level of access are based upon the Security Policy created by the Essex County Governing Committee. The Agency ILEI Liaison Officer certifies that the above mentioned User meets the qualifications described in the ILEI Security Policy, based upon personal review of the following:

- ☐ The User is a Full-time Law Enforcement Officer in good standing
- ☐ As a civilian police employee who has satisfied the ILEI Security Policy requirements based upon a review of a state and national criminal history check based on fingerprint identification

User Certification:

I, _____, [Name of Agency] ILEI User, acknowledge and certify that I have been trained in the use of the ILEI system.

Signature

Date

Agency ILEI Administrator Certification:

I, _____, ILEI Liaison Officer for the above mentioned agency verify the above named User meets the ILEI eligibility as specified in the Security Policy established by the Essex County ILEI Governing Committee.

Signature

Date