

# **LEIN Policy (sample document)**

## Index

Purpose	4
Definitions	5
Terminal Agency Coordinator (TAC)	7
Local Agency Security Officer (LASO)	9
Security	11
Training	14
Entries	15
Validation Procedures	16
Criminal History Record Information (CHRI)	19
Compliance	20
<b>Appendix</b>	21
MDC/MDT Usage	22
Acceptable Use Policy	24
Anti-Virus Guidelines	29
Disposal of Media Policy	31

Password Policy and Procedures	32
Unique Identifiers Policy and Procedure	37
Holder of the Record Agreement	38
Hit Confirmation Agreement	39
ORI Usage for Hot Files (Law ORI)	40
ORI Usage for Hot Files (Dispatch ORI)	41
Management Control Agreement IT	42
Rules of Behavior Form	44

I. Purpose

To establish procedures and guidelines for the proper operation of LEIN/NCIC system access, including all forms of connectivity and access. To assure compliance with laws, policies and rules enacted and adopted by Michigan State Police, LEIN Field Services and the Federal Bureau of Investigation, Criminal Justice Information Systems (FBI CJIS) National Crime Information Center (NCIC). To assure compliance with the documents incorporated in the LEIN User Agreement executed between this agency and Michigan State Police, LEIN Field Services.

## II. Definitions

Access: Access shall be defined as the ability to see, hear or read information obtained from LEIN/NCIC.

The use of the LEIN system and its capabilities is strictly for criminal justice use and not for personal information, personal gain or for release to non-authorized persons/agencies.

Only those authorized persons (terminal operators) who are trained in LEIN/NCIC standards and certified by this agency's Terminal Agency Coordinator (TAC) shall be allowed system access.

Law Enforcement Information Network (LEIN): The law enforcement computer system that allows criminal justice agencies in the State of Michigan to access various types and sources of law enforcement related information and to communicate directly with other criminal justice agencies. The LEIN computer, itself, contains all **Michigan** warrant, missing person, stolen, abandoned, and impounded vehicle information. In addition, it allows agencies access to the Secretary of State (SOS) computer, the National Crime Information Center (NCIC), the International Justice and Public Safety Network (Nlets), the Corrections Management Information System (CMIS), the Michigan Criminal History Record (CHR) system, and the Interstate Identification Index (III).

Local Agency Security Officer (LASO): All agencies that have direct access to the Law Enforcement Information Network (LEIN) shall appoint a security point of contact, known as a Local Agency Security Officer (LASO). The LASO can be, but is not required to be, the agency's Terminal Agency Coordinator (TAC).

Terminal Agency Coordinator (TAC): The TAC is the person designated by the Agency Head to be in charge of the LEIN system. The TAC is responsible for certifying operators, physical and technical security, monthly validations, LEIN audits and duties as delegated by the Michigan State Police (MSP), LEIN Field Services Section (LFSS). The TAC shall be knowledgeable in all aspects of LEIN/NCIC Policy and procedures, CJIS security and LEIN equipment.

Terminal: A terminal is any device used to access LEIN/NCIC information.

Terminal Operator: A terminal operator shall be any person that uses a terminal, as described above, to access LEIN/NCIC systems and data.

Validation: Validations are the process whereby all of an agency's LEIN/NCIC entries are checked periodically for accuracy, completeness, and that the complaint/warrant (source documentation) is still active. MSP LFSS provides

monthly computerized lists of LEIN/NCIC entries including validation instructions to the agency TAC to review for accuracy, completeness and validity (still active).

### III. Terminal Agency Coordinator (TAC)

- A. The agency shall have a minimum of one TAC and one alternate TAC, when possible.
- B. TACs shall be versed and knowledgeable in rules, regulations, applications, and operations of LEIN/NCIC and its interfaced systems. The TAC shall serve as liaison with LEIN Field Services Section on behalf of the agency head.
- C. The agency shall notify LFSS upon appointment, change or correction of a named individual to the TAC position.
- D. All agency TACs shall complete a LEIN TAC basic instruction school and are required to attend all LEIN TAC update classes, as scheduled.
- E. Responsibilities:
  - 1. Liaison: to serve as the main contact person for the agency for LEIN/NCIC issues and to maintain, update, distribute and post mailings and correspondence from LFSS.
  - 2. Compliance: to ensure the agency is compliant with all rules, regulations and system integrity, including LEIN/NCIC access, dissemination and security.
  - 3. Validation: to ensure the quality, timeliness and completeness of agency entries and cancellations through the monthly validations of record entries.
  - 4. Training: to coordinate and maintain training records of agency terminal operators and other agency practitioners.
  - 5. Certification: to conduct agency terminal operator certification and recertification testing. To enter, maintain, and update the LEIN certified operator file.
  - 6. Audit: participate in the agency triennial audit with LFSS audit staff.
- F. Duties:
  - 1. Agency ORI Listing: periodic review of the agency's ORI listing for currently active, in use, ORIs. Notify LFSS to retire any ORIs no longer active.

2. Policies: establish and maintain a LEIN/NCIC policy and procedures manual within the agency.
3. Violations: report all known violations to LFSS.
4. Forms: ensure that required forms and agreements are current and on file. These forms include but are not limited to: LEIN user agreement, fire department agreement, school access agreement, and holder of the record agreement.

#### IV. Local Agency Security Officer (LASO)

##### A. Responsibilities

###### 1. Point of Contact (POC):

The LASO serves as the single point of contact (POC) between MSP and this agency on network and security issues. The LASO is responsible for reporting violations of the security policy. The LASO serves as the POC for computer incident notification and distributing security alerts to this agency.

###### 2. Network

The LASO coordinates start-up and upgrades to the network and assists with making application to the state for MSP ISO approval. The LASO assists in maintaining network topology documentation which satisfy required security measures and provides guidance in implementing security measures.

###### 3. Procedures

The LASO assists with the development of written policy and procedures regarding termination of access for terminated employees. The LASO shall have documented procedures in place to monitor all security policies such as changing of passwords, log-ons, etc. The LASO will establish and follow a security incident violation response and reporting procedure to discover, investigate, document, and report on all security incidents/violations within this agency.

###### 4. Training

The LASO assists with the distribution of training manuals and other related publications to agency users. The LASO develops information security training programs and ensures all personnel have been properly trained. The LASO also conducts or assists with the presentation of such training programs. From time to time the LASO will provide security awareness briefings to agency. The goal of these briefings is to ensure that personnel are made aware of:

- Threats, vulnerabilities, and risks associated with accessing CJIS
- What requires protection
- Information accessibility, handling, marking, and storage considerations
- Physical and environmental considerations
- System, data, and access controls

- Contingency planning procedures
- Secure configuration control requirements
- Social engineering practices
- Responsibility to promptly report security violations to the LASO.

The LASO will assist with giving all new employees security awareness training within six months of their appointment or assignment, as part of their orientation. Continued training shall be provided whenever there is a significant change in the agency information systems security environment or procedures, or when an employee enters a new position. Refresher training shall be given biennially to all employees.

## V. Security

### A. Pre-Employment Requirements

A full and complete background investigation must be completed on all prospective agency employees. Pre-employment inquiries will be conducted by the agency on all persons who may have access to LEIN/NCIC materials. The background investigation should include the following queries:

- LEIN/NCIC wanted files
- Criminal history records (purpose code 52:J/Employee)
- Secretary of State complete driver's records
- Corrections Management Information Systems (CMIS)
- Livescan fingerprints

Any prospective employee with a felony or serious misdemeanor conviction or charge is prohibited from accessing LEIN/NCIC. Serious misdemeanor (93 day misdemeanor convictions) categories are: crimes against a person (including domestic violence), drug offenses, weapons offenses, and misdemeanor LEIN misuse conviction.

A full and complete background investigation will be repeated for every terminal operator once every five years.

### B. Escorted and Unescorted Visitor Access

All persons with access to areas containing CJIS equipment and/or printed/stored data shall be accompanied by appropriate staff at all times. This includes government officials, contractors, vendors, retired staff members, etc.

Unescorted access may be granted, for specific vendor or other work related service, once a fingerprint and background check, as described in section V.A., of the person is completed by the agency. This includes contracted support staff, IT support, volunteers, etc.

### C. User Accounts, Names and Passwords

All operators must be identified by unique user name and password. Operators cannot share a user account. User accounts must be locked after three (3) failed log in attempts. Passwords cannot be the same as the user name. Passwords require both numbers and letters. Passwords must have a minimum of eight characters. Users must be forced/prompted to change their passwords every 90 days. Users cannot reuse the last ten (10) passwords.

#### D. Printout Disposition

The TAC will ensure that printed LEIN/NCIC data information be disposed of properly through burning or the use of a crosscut paper shredder or licensed-bonded sensitive document refuse company, whose employees have been properly fingerprinted and criminal history background checked.

#### E. Faxing

Faxing of LEIN/NCIC material is allowable if the receiving fax machine is at an authorized agency and is attended by the appropriate staff.

#### F. E-mail

Must be encrypted.

#### G. Storage and Retention of LEIN/NCIC Data

LEIN/NCIC data, including electronic files and printed materials will not be held indefinitely. Once the information has been gleaned or the case files have been closed, the data must be purged or destroyed, unless the data is pertinent to the integrity of the case.

Stored data will be afforded the same security as system access areas with emphasis on security and limited access.

#### H. Radio Transmissions

All materials received via LEIN/NCIC terminals may be routinely transmitted via radio airwaves, except for Criminal History Records. Criminal History Records shall not be routinely transmitted via radio transmissions, however, are permissible, in part, for reasons of identification and officer and public safety.

#### I. Agency Security

This agency's facility, including satellites offices or other remote locations, and all related computer infrastructures which provide access to the CJIS network will have adequate physical security at all times to protect against any unauthorized access to or routine viewing of computer devices, access devices, and printed and stored data. Restricted and controlled areas will be prominently posted and separated from non-sensitive areas and non-

restricted and controlled areas by physical barriers that restrict unauthorized access. Every physical access point to this facility or restricted area housing information systems that access, process, or display CJIS data will be controlled and secured.

All LEIN terminals must be in a secure location under the direct management, control and supervision of authorized personnel. Terminals must be inaccessible to the public or persons not authorized to operate, view or possess LEIN/NCIC transmitted or received data.

J. Procedure for Updating networks, connectivity and terminals

Prior to any change, update, upgrade, or expansion of this agency's network, connectivity, access points, access type and fixed end equipment (terminals, mobiles, handheld devices, etc.), which impact the current LEIN approved network diagram are tested or implemented, appropriate documentation will be forwarded to LEIN Field Services for approval as compliant with FBI and Michigan CJIS Security Policy.

***To be used by Interface Provider Agencies:***

Prior to connecting an interface subscriber to this agency's access to LEIN/NCIC, said subscriber agency must provide a LEIN approved network diagram.

K. Procedures for Adding/Removing Users

***Under this section please describe the process you use to accomplish adding and removing users from your system. If you are the interface provider, describe the procedure as it relates to your subscriber agencies also.***

## VI. Training

### A. Certification

The TAC will be responsible for training and testing all operators to certify their proficiency. Training requirements will include those items stipulated in the LEIN TAC manual Chapter 11. New or reassigned employees must be tested within six months of hire or reassignment.

### B. Recertification

The TAC will be responsible for the recertification of terminal operators every two years. All terminal operators must pass a written test with a minimum score of 70%.

### C. Security Awareness

The LASO will be responsible for providing security awareness training to all operators and IT staff within the first six months of hire. Updated security awareness training will be provided to all operators and IT staff every two years.

### D. Documentation

This agency will maintain documentation pertaining to the training materials used, including test results, and those employees who received training. Each employee will sign a Rules of Behavior form upon completion of security awareness training.

## VIII. Entries

### A. Timely

All entries shall be entered into LEIN/NCIC as soon as physically possible after receiving the complaint/court order. NCIC requires all entries within 72 hours of being received/reported.

### B. Accurate/Second Party Checks

It will be the responsibility of the TAC to insure all LEIN/NCIC entries are checked by a second party for validity, accuracy and completeness within 48 hours of the entry.

### C. Complete/Packing Records

Operators will make every effort to add additional identifiers for all LEIN/NCIC entries by checking the complaint report, SOS records, CCH identifiers, CMIS records and agency records to assure completeness and accuracy of entries. License plate and VIN's should be verified with a LEIN/SOS query. This agency will only use packing data which has been verified from a reliable source and not copied from another agency's LEIN entry.

*(This section is optional, to be included only if applicable to the agency)*

### D. Court Entered Warrants

Once a warrant has been entered by the court it is the responsibility of this agency to verify the accuracy of the entry and to pack the warrant with additional identifiers and information to effect an arrest

## IX. Validation Procedures

To facilitate file accuracy, the agency head shall:

1. Ensure that validation is accomplished forthwith. Validation obliges this agency to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current support documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files or other appropriate source or individual. In the event this agency is unsuccessful in its attempts to contact the victim, complainant, etc., a determination will be made based on the best information and knowledge available whether or not to retain the original entry in the file.
2. Assign a specific supervisor or Terminal Agency Coordinator (TAC) to assume responsibility for the validation processes. Upon receiving validation lists, it is absolutely necessary that this agency check thoroughly to be certain that the entries are active and current.
3. Establish good administrative check procedures within the agency to insure that entries and cancellations are properly made.
4. Wherever possible, maintain warrant and vehicle files in a location easily accessible to LEIN operators.
5. Confirm all hits with the entering jurisdiction.
6. Ensure that terminals are operated by thoroughly trained, competent personnel.
7. The completed validation reports must be retained from the most current year plus one (maximum 24 months total). These reports may be used in the LEIN audit process and will be available to the LEIN auditor for review.

### VALIDATION PROCEDURES

These procedures must be followed to meet the LEIN/NCIC validation requirements. Cancel or correct/modify records as needed.

### **Wanted Persons and Orders entered by Law Enforcement Agencies**

1. For each record appearing on the validation listing, an inquiry will be made into LEIN to verify the existence of the warrant/order in LEIN. Verify with the court records to ensure the order is still valid.

2. Establish a warrant recall procedure with the issuing court to ensure that the court does not cancel a warrant and fail to notify the entering agency.
3. For each record appearing on the validation listing, an inquiry will be made into LEIN to compare the individual fields with the warrant/order to verify they are accurate and complete. Check the LEIN/NCIC and other supplemental documentation for additional information to “pack” the record.
4. For an extraditable offense, contact the Prosecutor to review the extradition limitations.
5. Make every effort to obtain all known identifiers to pack the warrant.

### **Wanted Persons entered by Courts**

Either manually view the case jacket or perform an electronic check to match with the LEIN files to ensure the record is correct and valid

### **Missing Persons**

1. Verify the existence of documentation and signature authorizing the entry (required, except missing persons under 21 years of age).
2. Contact the complainant (authorizing parent, guardian, or other reporting person) of the missing person, to verify subject is still missing and to obtain any additional information.
3. For each record appearing on the validation listing, an inquiry will be made into LEIN and the individual fields compared with the missing person report to verify the information is accurate and complete.
4. Contact the Investigating Officer or any other law enforcement agencies involved in the case for updated information.
5. Ensure dental records are entered. All missing persons over 30 days are required to have dental records entered, pursuant to MCL 333.2844A, P.A. 1986.

### **Unidentified Persons**

1. Verify the existence of documentation and signature authorizing the entry.
2. Contact the authorizing reporting person on the unidentified person, to verify subject is still unidentified and any additional information.
3. For each record appearing on the validation listing for the first time, an inquiry will

be made into NCIC to compare the individual fields with the unidentified person report to verify they are accurate and complete.

4. Contact the Investigating Officer or any other law enforcement agencies involved in the case for updated information.

## **Property**

Property includes vehicles, vehicle and boat parts, boats, license plates, guns and securities.

1. Verify the existence of the record in LEIN/NCIC with the original report.
2. For each record appearing on the validation listing for the first time, an inquiry will be made into LEIN/NCIC to compare the individual fields with the report to verify they are accurate and complete.
3. Contact the complainant, victim, insurance company, or investigating officer to verify the record is still outstanding.

## **MINIMIZE LITIGATION**

The procedures outlined in this section will serve to minimize the potential litigation for this agency, resulting from arrests made due to inaccurate or obsolete information.

## **CERTIFICATION REQUIREMENTS**

This agency is required to certify the validity of our entries as per the aforementioned schedule. Within 30 days of receipt of a validation list, or prior to the deadline as indicated by LEIN Field Services, the agency head or authorized representative is required to certify via a LEIN VLN transaction that all records on the monthly validation list are valid, accurate and complete.

Since a validation listing may be received every 30 days, two validation listings could be on hand at one time.

Failure to certify the validity of this agency's records prior to the deadline as indicated by LEIN Field Services will result in those records being removed from the LEIN/NCIC files by LEIN Field Services.

In instances where this agency requires more than 30 days in which to validate our entries, reasonable time extensions may be approved by the State of Michigan CJIS Systems Officer (CSO).

## IX. Criminal History Record Information (CHRI)

LEIN/NCIC access to Criminal History Records is permitted only under the management control of criminal justice agencies in the discharge of their official, mandated responsibilities. Personal use of criminal history record information is strictly prohibited.

Criminal History Records inquiries must be supported by paper or electronic documentation. Examples are:

- Incident Reports
- Officer Daily Log
- Radio Log/Recording
- Arrest Documentation
- Electronic readily retrievable data bases
- Application
- Officer Notebook
- Civil Infractions

### Secondary Dissemination

All Criminal History Records forwarded to an authorized user/agency (i.e. prosecutor, court, another law enforcement agency) will be documented in a supplement report or paper log. Documentation will include the date of dissemination, the name of the person receiving the information and the name of the authorized agency.

## X. Compliance

Misuse of LEIN violates MCL 28.214 Section 4 of the LEIN Policy Council Act, amended effective February 1, 2006.

### Sec. 4

- (3) A person shall not access, use, or disclose nonpublic information governed under this act for personal use or gain.
- (5) A person shall not disclose information governed under this act in a manner that is not authorized by law or rule.
- (6) A person who intentionally violates subsection (3) or (5) is guilty of a crime as follows:
  - (a) For a first offense, the person is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than \$500.00, or both.
  - (b) For a second or subsequent offense, the person is guilty of a felony punishable by imprisonment for not more than 4 years or a fine of not more than \$2,000.00, or both.

Misuse of SOS records violates the Driver Policy Protection Act.

### Sec. 903 (1)

- A. A person who makes a false certification to access personal information is guilty of a felony.
- B. Any individual who uses personal information for a reason other than a permissible purpose commits a felony.

Any officer or civilian employee of this agency who violates any section of this policy, LEIN Policies published in the LEIN manual, state or federal statute subjects themselves to agency discipline, up to and including termination. TAC's must report any suspected violation in writing to the Agency Head and LEIN Field Services Section.

# Appendix

**APPENDIX 1**  
**MDC/MDT USAGE**

*(This section is optional, to be included only if applicable to the agency)*

Definitions:

1. MDC – a mobile data computer
2. MDT – a mobile data device.

Usage:

- A. Only agency personnel trained, tested, and assigned to operate MDC's shall be authorized to utilize this terminal equipment. Persons who are not certified as LEIN terminal operators are not permitted to operate MDC's that are able to access LEIN/NCIC.
- B. The policies governing access, usage, release of information, content, format and other applicable guidelines established by LEIN/NCIC shall be strictly adhered to.
- C. MDC's are to be used for law enforcement related duties only and in accordance with LEIN/NCIC regulations. MDC's are subject to the same security and operational rules and policies as "in house" or fixed desktop devices.
- D. LEIN/NCIC Hits received on the MDC must be confirmed.
- E. Each user shall be required to log on the MDC at the beginning of their shift and to log off MDD at the completion of their time on patrol.
- F. Each user shall be uniquely identified in LEIN/NCIC by username and password. Users may not use another user's username and their password must be not be known to any other user.
- H. Users are required to blank or close the MDC screen when exiting the vehicle, or when unauthorized persons are occupying the vehicle.

## **Appendix 2** **Acceptable Use Policy**

*This document is required by LEIN/ NCIC*

### **1.0 Overview**

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to <Agency Name> established culture of openness, trust, and integrity. <Agency's Security Team> is committed to protecting <Agency Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, File Transfer Protocol, and National Crime Information Center access are the property of the <Agency Name>. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every <Agency Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

### **2.0 Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at <Agency Name>. These rules are in place to protect the employee and <Agency Name>. Inappropriate use exposes <Agency Name> to risk including virus attacks, compromises of the network systems and services, and legal issues.

### **3.0 Scope**

This policy applies to employees, contractors, consultants, temporary staff, and other workers at <Agency Name>, including all personnel affiliated with LEIN/NCIC and third parties. This policy applies to all equipment that is owned or leased by <Agency Name>.

### **4.0 Policy**

#### **4.1 General Use and Ownership**

1. While <Agency Name's> network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the <Agency Name>. Because of the need to protect <Agency Name's> network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Agency Name>.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or management.
3. <Agency Name> security department recommends that any information that a user considers sensitive or vulnerable (etc. residual LEIN/NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted. For guidance on information classification, see <Agency Name> Information Classification Policy.
4. For security and network maintenance purposes, authorized individuals within <Agency Name> may monitor equipment, systems and network traffic at any time, per <Agency Name> Audit Policy>.
5. <Agency Name> reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

## **4.2 Security and Proprietary Information**

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: LEIN/NCIC information, state criminal history information, agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Please review <Agency Name's> Password Policy for guidance.
3. All personal computers, laptops, and workstations should be secured with password-protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off (control-alt-delete) when the computer is unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with "Laptop Security Policy".
5. All devices used by employees that are connected to the <Agency Name> Internet/Intranet/Extranet, whether owned by the employee or <Agency

Name>, shall be continually executing approved virus-scanning software with a current database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

### **4.3 Unacceptable Use**

The following activities are, in general, prohibited. Under no circumstances is an employee of <Agency Name> authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing <Agency Name> owned resources. The list below is by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

Misuse of LEIN violates MCL 28.214 Section 4 of the LEIN Policy Council Act, amended effective February 1, 2006.

#### **Sec. 4**

- (3) A person shall not access, use, or disclose nonpublic information governed under this act for personal use or gain.
- (5) A person shall not disclose information governed under this act in a manner that is not authorized by law or rule.
- (6) A person who intentionally violates subsection (3) or (5) is guilty of a crime as follows:
  - (a) For a first offense, the person is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than \$500.00, or both.
  - (b) For a second or subsequent offense, the person is guilty of a felony punishable by imprisonment for not more than 4 years or a fine of not more than \$2,000.00, or both.

Misuse of SOS records violates the Driver Policy Protection Act.

#### **Sec. 903 (1)**

- A. A person who makes a false certification to access personal information is guilty of a felony.
- B. Any individual who uses personal information for a reason other than a permissible purpose commits a felony.

#### 4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized access, copying, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.).
2. Installation of any copyrighted software for which <Agency Name> or end user does not have an active license is strictly prohibited.
3. Installation of any software without pre-approval and virus scan is strictly prohibited.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to <Agency Name> Security administration.
8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network, or account.
10. Interfering with or denying service to any user other than the employee's host.
11. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
12. Providing information about LEIN/NCIC or list of <Agency Name> employees to parties outside <Agency Name>.

## 5.0 Enforcement

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

I have read, acknowledge, and will abide by the information obtained in this document.

**User (Print Name):** \_\_\_\_\_

**Date:**

**User Signature:** \_\_\_\_\_

**Date:**

## **Appendix 3** **Anti-Virus Guidelines**

*This document is required by LEIN/NCIC*

### **1.0 Purpose**

To establish requirements which must be met by all computers connected to <Agency Name> networks to ensure effective virus detection and prevention.

### **2.0 Scope**

This policy applies to all <Agency Name> computers that are PC-based or use PC-file directory sharing. This includes, but is not limited to, desktop computers, file/ftp/tftp/proxy servers, and any PC-based equipment.

### **3.0 Policy**

All <Agency Name> PC-based computers must have <Agency Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. <Agency Name>'s information security team has recommended the following processes to ensure that anti-virus software is run at regular intervals, and to keep computers virus-free.

Recommended processes to prevent virus problems:

- Always run the corporate standard.
- Run the current version and install anti-virus software updates as they become available.
- Anti-virus software is to be enabled on all workstations and servers at start-up and employ resident scanning.
- Detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways.
- On servers, update virus signatures files immediately, or as soon as possible, with each new release.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk-sharing with read/write access unless there is absolutely an agency requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Always scan any media that is brought into the agency before introducing it to the network.

Any activities with the intention to create and/or distribute malicious programs into <Agency Name>'s networks (e.g., viruses, worms, Trojan horses logic bombs, etc.) are prohibited. Virus-infected computers must be removed from the network until they are verified as virus-free. If a virus is detected on your workstation and the anti-virus software can not eliminate the virus, please contact <Agency Representative>. **DO NOT TURN OFF** your computer, it will be quarantined and taken off of the network until it can be scanned and re-imaged with the operating system image.

#### **4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## **Appendix 4**

### **Disposal of Media Policy and Procedures**

*This document is required by LEIN/NCIC*

#### **1.0 Purpose**

The purpose of this policy is to outline the proper disposal of media at <Agency Name>. These rules are in place to protect sensitive and classified information, employees and <Agency Name>. Inappropriate disposal of <Agency Name> and LEIN/NCIC and FBI information and media may put employees, <Agency Name> and the FBI at risk.

#### **2.0 Scope**

This policy applies to employees, contractors, temporary staff, and other workers at <Agency Name>, including all personnel with access to sensitive and classified data and media. This policy applies to all equipment that processes classified and sensitive data that is owned or leased by <Agency Name>.

#### **4.0 Policy**

When no longer usable, diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items used to process or store classified and/or sensitive data shall be properly disposed of in accordance with measures established by <Agency Name>. The following procedures will be followed:

- When no longer usable, hard copies and print-outs shall be placed in properly marked shredding bins.
- Diskettes and tape cartridges shall be taken apart and placed in the properly marked shredding bins.
- After media has been shredded it will be placed in appropriate bins to be incinerated or disposed of properly.

IT systems that have processed, stored, or transmitted sensitive and/or classified information shall not be released from <Agency Name's> control until the equipment is sanitized and all stored information has been cleared. For sensitive, but unclassified information, the sanitization method shall be approved by <Agency Name>. For classified systems, National Security Association approved measures shall be used. The following procedures will be followed:

- Employees will send all hardware that processes and/or stores

classified and/or sensitive data to <Agency Name> <Security Personnel> to be properly disposed.<Agency Name> <Security Personnel> will dispose of hardware by one of the following methods:

- **Overwriting** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. The number of times the media is overwritten depends on the level of sensitive information.
- **Degaussing** - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
- **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc.

Also, computers that are used to transmit classified and/or sensitive information must protect residual data. This can be accomplished with the use of integrated encryption technology. This technology uses a device or software which encrypts all data as it is written to the disk. When the user retrieves a file, the data is automatically decrypted for the owner to use. This encryption/decryption process is typically transparent to the user. Should the hard drive be removed, no useable data can be retrieved.

#### **4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix 5  
**Password Policy and Procedures**

*This document is required by LEIN/NCIC*

## **1.0 Overview**

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of <Agency Name>'s entire network. As such, all <Agency Name> employees (including contractors and vendors with access to <Agency Name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

## **2.0 Purpose**

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

## **3.0 Scope**

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Agency Name> facility, has access to the <Agency Name> network and/or LEIN/NCIC network, or stores any non-public <Agency Name> information.

## **4.0 Policy**

### **4.1 General**

- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
- All production system-level passwords must be part of the Information Security administrated global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts with access to LEIN/NCIC privileges must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of

electronic communication.

- Where simple network management protocol (SMTP) is used, the community strings must be defined as something other than the standard defaults of “public,” “private,” and “system” and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level, system-level, and LEIN/NCIC access level passwords must conform to the guidelines described below.

## 4.2 Guidelines

### General Password Construction

Passwords are used for various purposes at <Agency Name>. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., Dynamic passwords which are used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Name of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites companies, hardware, software.
  - The words “<Agency Name>,” “WVSP,” “HPD,” “CKSFP” or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, 111222, zyxwvts, 4654321, etc.
  - Any of the above spelled backward like nhoj, yrrehckcalb, yffulf, etc.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#%&^\*()\_+{}[]:";<>?,.?
- Are at least eight alphanumeric characters long.
- Are not a word within any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. **NOTE: Do not use either of these examples as passwords**

### 4.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her point-of-contact (POC).
- Supervisor or POC should fill out a password deletion form and send it to <Agency's POC>.
- <Agency's POC> will then delete the user's password and delete or suspend the user's account.
- A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.
- The password deletion form will be filed in a secure filing system.

#### 4.4 Password Protection Standards

Do not use your user id as your password. Do not use the same password for <Agency Name> accounts as for LEIN/NCIC accounts. For example, select one password for your Windows account login and a different one for your NCIC account login. Do not share <Agency Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <AgencyName> information.

Here is a list of “do not’s”

- Don’t reveal a password over the phone to anyone
- Don’t reveal a password in an mail message
- Don’t reveal a password to the boss
- Don’ talk about a password in front of others
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share a password with family members
- Don’t reveal a password to a co-worker while on vacation
- Don’t use the "Remember Password" feature of applications
- Don’t write passwords down and store them anywhere in your office.
- Don’t store passwords in a file on ANY computer system without encryption.

If someone demands a password, refer them to this document or have them call <list name of Information Security Officer (ISO) or Agency POC.

If an account or password is suspected to have been compromised, report the incident to <Name of ISO or POC> and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the FBI or <Agency Security Department or POC>. If a password is guessed or cracked during one of these scans, the user will be required to change it.

#### C. Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide some sort of role management, such that one user can take over the function of another without having to know the other’s password.
- Should support Terminal Access Controller Access Control System+

## **D. Remote Access Users**

Access to the <Agency Name> networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

## **5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## **Appendix 6**

### **Unique Identifier Policy and Procedures**

*This document is required by LEIN/ NCIC*

#### **1.0 Purpose**

The purpose of this policy is to ensure accountability of all users that access <Agency Name> network and network devices.

#### **2.0 Scope**

The scope of this policy is to define the creation of a unique identifier for individuals that access <Agency Name> network, network devices and LEIN/NCIC information.

#### **3.0 Policy**

##### **3.1 General**

<Agency Name> requires that each employee that has access to <Agency Name> network, applications, and/or LEIN/NCIC for the purpose of storing, processing, and/or transmitting information shall be uniquely identified by use of a unique identifier. A unique identifier shall also be required for all persons who administer and maintain the system(s) that access agency and LEIN/NCIC information and/or network. <Agency Name> requires users to identify themselves uniquely before the user is allowed to perform any action on the network and/or applications. All user IDs shall belong to currently authorized users. Identification data shall be kept current by adding new users and disabling former users. Employees shall not share their IDs with other employees, supervisors, management, or family members at any time.

##### **3.2 Guidelines**

The unique identification can take the form of the following examples:

- User's full name (JohnWDoe)
- Form of full name (SASmith)
- Badge number (WV724966)
- Combination of name and badge number (jhardWV966)
- Serial Number (123456789)
- Other unique alphanumeric identifier

#### **4.0 Enforcement**

Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, and termination of employment.

**Holder of the Record Agreement  
(SAMPLE)**

This Agreement, dated \_\_\_\_\_, shall satisfy the National Crime Information Center (NCIC) requirement to define a HOLDER OF THE RECORD in cases where the Originating Agency Identifier (ORI) on a record entered into the LEIN/NCIC is not the ORI of the entering agency.

This Agreement is between \_\_\_\_\_  
(Non-Entering Agency) whose ORI is \_\_\_\_\_ and  
\_\_\_\_\_ (Entering Agency) whose ORI is  
\_\_\_\_\_ and defines \_\_\_\_\_  
(Entering Agency) as the HOLDER OF THE RECORD.

Further, this Agreement delineates that the HOLDER OF THE RECORD shall be responsible for entering, updating, modifying, "packing", confirming hits, validating and canceling all records entered into the LEIN/NCIC on behalf of the above, non-entering agency, 24 hours per day, seven days per week. All records will be date/time stamped upon receipt and will be entered into the LEIN/NCIC according to timeliness standards set forth by LEIN/NCIC. Under no circumstances does this Agreement relieve the above, non-entering agency of their responsibility, as defined by LEIN/NCIC, for the accuracy and content of records entered into LEIN/NCIC.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Agency)

\_\_\_\_\_  
(Printed name)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Agency)

\_\_\_\_\_  
(Printed name)

\_\_\_\_\_  
(Date)

**Hit Confirmation Agreement  
(SAMPLE)**

This Agreement is between \_\_\_\_\_  
(Confirming Agency), whose ORI is \_\_\_\_\_, and  
\_\_\_\_\_ (Record Entering agency),  
whose ORI is \_\_\_\_\_.

Further, this Agreement delineates that the Confirming Agency shall be responsible for responding to all hit confirmation requests on behalf of the Record Entering Agency, for all records entered into the LEIN/NCIC by the Record Entering Agency, between the hours of \_\_\_\_\_ and \_\_\_\_\_, \_\_\_\_\_ (days of the week), to ensure 24/7 hit confirmation coverage. All responses to hit confirmation requests will be made according to LEIN/NCIC Hit confirmation requirements as set forth in the LEIN Operations Manual and the NCIC Operating Manual.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Agency)

\_\_\_\_\_  
(Printed name)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Agency)

\_\_\_\_\_  
(Printed name)

\_\_\_\_\_  
(Date)

**Sample Agreement Template – Law ORI**

Use of \_\_\_\_\_ (Law Enforcement Agency) ORI  
for \_\_\_\_\_ (Dispatch Agency) Hot File Inquiries

The \_\_\_\_\_ (Law Enforcement Agency)  
authorizes \_\_\_\_\_ (Dispatch Agency)  
to utilize Originating Agency Identifier (ORI) \_\_\_\_\_ (Law Enforcement  
Agency ORI) for the purpose of pre-screening calls for service, when deemed necessary  
by dispatch personnel. Information obtained through such inquiries shall only be  
provided to authorized criminal justice personnel.

Examples of usage include, but are not limited to: warrant checks on subjects involved in  
domestic or other potential call for service; registration/file check on a  
suspicious/abandoned vehicle, etc.

Circumstances of usage include, but are not limited to: a law enforcement officer has not  
yet been assigned to the call for service; suspect status must be confirmed in order to  
process a call for service; with the goal of optimum performance as well as efficiency and  
prioritization of services.

This agreement shall be re-executed should the undersigned person(s) change.

\_\_\_\_\_  
Law Agency Head Name/Signature  
Law Enforcement Agency Name

\_\_\_\_\_  
Dispatch Agency Head Name/Signature  
Dispatch Agency Name

Date Executed: \_\_\_\_\_

**Sample Agreement Template- Dispatch ORI**

Use of \_\_\_\_\_ (Dispatch Agency) ORI  
for \_\_\_\_\_ (Law Enforcement Agency) Inquiries

The \_\_\_\_\_ (Law Enforcement Agency)  
authorizes \_\_\_\_\_ (Dispatch Agency)  
to utilize Originating Agency Identifier (ORI) \_\_\_\_\_ (Dispatch Agency ORI)  
for the purpose of pre-screening calls for service, when deemed necessary by dispatch  
personnel. Information obtained through such inquiries shall only be provided to  
authorized criminal justice personnel.

Examples of usage include, but are not limited to: warrant checks on subjects involved in  
domestic or other potential call for service; registration/file check on a  
suspicious/abandoned vehicle, etc.

Circumstances of usage include, but are not limited to: a law enforcement officer has not  
yet been assigned to the call for service; suspect status must be confirmed in order to  
process a call for service; with the goal of optimum performance as well as efficiency and  
prioritization of services, call volume and workload preclude dispatch staff from  
performing these queries under the individual law enforcement agency's ORI, etc.

This agreement shall be re-executed should the undersigned person(s) change.

\_\_\_\_\_  
Law Agency Head Name/Signature  
Law Enforcement Agency Name

\_\_\_\_\_  
Dispatch Agency Head Name/Signature  
Dispatch Agency Name

Date Executed: \_\_\_\_\_

**MANAGEMENT CONTROL AGREEMENT**  
**(template)**  
**Between the**  
***(criminal justice agency name here)***  
**And the**  
***(information technology dept. name here)***

**1. PURPOSE**

The purpose of this Management Control Agreement (MCA) between \_\_\_\_\_ and \_\_\_\_\_ is to enumerate the terms, conditions, duties and responsibilities of each entity regarding the installation, operation and maintenance of criminal justice information technology located at \_\_\_\_\_. Additionally, to provide appropriate security for state and federal criminal justice systems under the supervision of \_\_\_\_\_.

**2. SCOPE**

The MCA applies to all systems and networks supporting the data of \_\_\_\_\_. Security shall include consideration of personnel, site, system and data.

**3. RESPONSIBILITIES**

**A. Personnel**

A background investigation including state and federal fingerprint-supported criminal history record checks, checks against state and national fugitive files must be completed for each prospective employee who may become and authorized user and operate or have access to systems and data.

Review of criminal history of persons arrested for a felony or high misdemeanor offense will disqualify a person from becoming an authorized user and operating or having access to systems and data.

A current list of authorized users will be maintained by \_\_\_\_\_.

**4. SECURITY**

**A. Site Security**

To the extent possible, all computer components and peripherals physically or logically connected to systems and data must be partitioned from non-criminal justice systems and data. Systems and data must be screened against unauthorized access, use and observation. Where systems and data are not

situated in a separate, dedicated area, staff in such areas will be screened in accordance with all applicable policies.

**B. System Security**

Access to systems and data is permitted for the scope of work that is necessary in connection with the operation, support and maintenance of such systems.

**C. Data Security**

\_\_\_\_\_, shall provide for the secure storage and/or disposal of all hardware, including drives and other media associated with CJIS data.

**5. AGREEMENT PERIOD**

The MCA remains in full force and effect, unless jointly terminated by both parties. The MCA may be modified upon joint agreement of both parties.

It is hereby agreed that the terms and conditions contained in this Management Control Agreement have been accepted by the officials signed names below, who are bound by the terms and conditions of this MCA.

\_\_\_\_\_  
(Criminal Justice Agency Rep)

Date:

\_\_\_\_\_  
(IT Rep)

Date:

## **User Rules of Behavior Acknowledgment Form**

As a user of an IT system, I acknowledge my responsibility to conform to the following requirements and conditions as directed by all relevant Information Assurance and Information Security Policies, Procedures and Guidelines. These conditions apply to all personnel who have access to FBI CJIS systems and all appropriate IT personnel.

1. I understand that failure to sign this acknowledgment will result in denial of access to FBI CJIS systems, terminal areas, and facilities that have FBI CJIS network equipment.
2. I acknowledge my responsibility to use the network only for official business except for such personal use involving negligible cost to the agency and no interference with official business as may be permissible under the acceptable use policy.
3. I understand that the network operates at a Sensitive but Unclassified level. I have all clearance necessary for access to the network, and will not introduce or process data that the network is not specifically designed to handle as specified by the Security Policy.
4. I understand the need to protect my password at the highest level of data it secures. I will NOT share my password and/or account. I understand that neither the Security Administrator/System Administrator, nor the Network Operations Center (NOC) will request my password. I will change my password at least every 90 days or as requested for security reasons.
5. I understand I am responsible for all actions taken under my account. I will not attempt to "hack" the network or any connected information system (IS), or attempt to gain access to data for which I am not specifically authorized.
6. I understand my responsibility to appropriately protect all output generated under my account, to include printed material, magnetic tapes, floppy disks, CD-ROMs, and downloaded hard disk files. I understand that I am required to ensure all hard copy material and magnetic media is properly labeled as required by policies and regulations.
7. I understand my responsibility to report all IS or network problems to my security Point Of Contact (POC). I will NOT install, remove, or modify any hardware or software.
8. I acknowledge my responsibility to not introduce any software or hardware not acquired and approved through the IT Security group. I also acknowledge my responsibility to have all official electronic media virus-scanned by the IT Security group before introducing it into the IS or network.
9. I acknowledge my responsibility to conform to the requirements of the Rules of Behavior, Acceptable Use Policy, and Security Policies and Procedures. I also

acknowledge that failure to comply with these policies and procedures may constitute a security violation resulting in denial of access to the IS, network, or facilities, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.

- 10. I agree that I have no expectation of privacy in any equipment or media I use. I consent to inspections by authorized agency personnel, at any time and agree to make any equipment available for audit and review by FBI personnel upon request.
- 11. I further consent that my use of FBI CJIS systems within agency owned or leased space is subject to system monitoring.
- 12. I have completed the required biennial Security Awareness Training required by the *CJIS Security Policy* for individuals managing or accessing FBI CJIS systems and/or data.

**User (Print Name):** \_\_\_\_\_ **Date:**

**User Signature:** \_\_\_\_\_ **Date:**

**LASO/Security Officer:** \_\_\_\_\_ **Date:**