POLICY & PROCEDURE

ELKHART LAKE POLICE DEPARTMENT

SUBJECT: **CRIMINAL RECORDS/TIME SYSTEM**

SCOPE: All Sworn Personnel

DISTRIBUTION: Policy & Procedure Manual

REFERENCE: WI State Statutes: 165.83, 165.84
TIME Operator Manual,
TIME System Security Manual

NUMBER: 10.02
ISSUED: 06/01/2015
EFFECTIVE: 07/15/2015
□ RESCINDS
□ AMENDS
WILEAG 4TH EDITION
STANDARDS: 9.1.9, 10.1.10

INDEX AS: CIB System Procedures
TIME System
Warrant Procedures with the TIME System

PURPOSE: The purpose of this Policy & Procedure is to establish the responsibilities and procedures to be followed in the use of the teletype system for the Elkhart Lake Police Department.

This Policy & Procedure consists of the following numbered sections:

I. DEFINITIONS

II. POLICY

III. TERMINAL OPERATORS

IV. VALIDATION OFFICER

V. ENTRY/CANCELLATION

VI. RECOVERY OF ITEMS (VEHICLES, SECURITIES, BOATS, ARTICLES, GUNS)

VII. CRIMINAL HISTORY RECORD INFORMATION

VIII. DEPARTMENT OF TRANSPORTATION INFORMATION

IX. DEPARTMENT OF MOTOR VEHICLE INFORMATION

X. ADMINISTRATIVE MESSAGES

XI. TIME SYSTEM SECURITY PROCEDURES

I. DEFINITIONS

For the purpose of this Policy & Procedure, the following definitions shall apply:

A. CHRI: Criminal History Record Information

B. CIB: Crime Information Bureau

C. CONTROL NUMBER: Number assigned to entries into TIME System from the Index File

D. DOT: Department of Transportation

E. DMV: Department of Motor Vehicles

F. GEOPICUP: Geographical Pick-up Warrant Restrictions

G. INDEX FILE: File maintained in the records division to index and record entries/cancellations into TIME System

H. III: Interstate Identification Index

I. NCIC: National Crime Information Center

J. NLETS: National Law Enforcement Telecommunications System

K. ORICASNO: Originating Agency Case Number

L. TIME: Transaction Information for Management of Enforcement

M. TSCC: TIME System Control Center

II. POLICY

A. It is the policy of the Elkhart Lake Police Department to participate in the Wisconsin Crime Information Bureau (CIB) System.

B. The TIME System is a computerized communications and data entry-retrieval system serving law enforcement agencies providing statewide and nationwide access to information: wanted persons, stolen vehicles, stolen articles, driver's license, and vehicle registration. The system also provides an effective method of administrative communication for law enforcement purposes. The Elkhart Lake Police Department, as a subscriber/user of the system, has agreed to utilize the system for official purposes only.

C. The TIME System shall be operated in compliance with Wisconsin Statutes 165.83 and 165.84 and shall be used for official law enforcement purposes as set forth in the TIME Operator's Manual and as described in this Policy & Procedure.

III. TERMINAL OPERATORS

A. Terminal operators will have completed the CIB Training Program and shall be certified by the State of Wisconsin to operate the TIME System for the express purposes of entry/modification/cancellation of wanted persons and stolen items (motor vehicles, boats, guns, securities and other articles, which may be entered into the system).

B. Terminal Operators shall be available 24 hours a day, seven days a week to access the TIME System to send and receive information. They shall also have 24 hours a day access to the Department's warrant and wanted person's information.

IV. VALIDATION OFFICER

A. The Validation Officer or TAC shall be responsible for file validations to insure that records in the computer files entered by the Department are accurate, complete and up-to-date.

B. Upon receiving validation printouts for entry classifications as provided by CIB, the Validation Officer or TAC shall insure that entries are validated and shall return the Certification Letter to CIB by the validation due date.

C. The Validation Officer or TAC shall be responsible for the quality control of the local TIME operations and shall cause periodic local accuracy checks of the system to be conducted independent of CIB mandatory validations. The Validation Officer or TAC shall be responsible for responding to any questionnaires or other correspondence from CIB, including CJIS Policy.

D. The Validation Officer or TAC shall be responsible to review this Policy yearly to ensure the agency meets all CIB/CJIS requirements.

V. ENTRY/CANCELLATION

A. All entries and cancellations shall be handled by the Sheboygan County Sheriff's Office, incident numbers will be assigned in accordance with the Policy & Procedure 10.03: Open Records.

VI. RECOVERY OF ITEMS (VEHICLES, SECURITIES, BOATS, ARTICLES, GUNS)

A. Queries will be made of the system on any item recovered by a member of the Elkhart Lake Police Department by the Sheboygan County Sheriff's Office.

B. Members of the Department who either recover or are notified of the recovery of any item having been reported to the Department as stolen/missing and entered into the TIME System, shall be responsible to notify the Sheboygan County Sheriff's Office to ensure that the item is removed from the system.

C. The notification and cancellation of recovered items is paramount in maintaining the integrity of the system and in minimizing the Department's liability.

VII. CRIMINAL HISTORY RECORD INFORMATION

A. The CHRI program within the TIME System provides for the exchange of criminal history information on individuals intrastate and interstate.

B. NLETS has a prescribed policy pertaining to CHRI which complies with the U.S. Department of Justice Rules & Regulations. Terminal operators will familiarize themselves with the NLETS policy as provided in the TIME Operator's Manual. NLETS policies apply to all Wisconsin law enforcement agencies.

C. The Elkhart Lake Police Department will make only authorized CHRI requests.

D. All CHRI requests will be made using the proper message key (format). Do not use an administrative message for CHRI requests.

VIII. DEPARTMENT OF TRANSPORTATION INFORMATION

A. Members of the Elkhart Lake Police Department will not directly disclose driver's license information (status/record) to any person other than a court, district attorney, county corporation counsel, Village attorney, or law enforcement agency.

B. Driver's license information received through the TIME System pertaining to JUVENILES contains information that is by statute confidential, not to be given to the public. This information is to be used for internal use of law enforcement agencies only.

C. Individuals requesting information on their own driver's license (status/record) and requesting a copy of same, will be referred to the Department of Transportation Office, Driver's License Section, Madison, Wisconsin.

IX. DEPARTMENT OF MOTOR VEHICLE INFORMATION

A. Members of the Elkhart Lake Police Department will not disclose motor vehicle registration information to any person other than a court, district attorney, county corporation counsel, and city attorney or law enforcement agency.

B. Individuals requesting motor vehicle registration information will be referred to the Department of Transportation, Motor Vehicle Registration Section, Madison, Wisconsin.

C. The Chief of Police or designee may authorize the release of motor vehicle registration information on an individual case basis.

X. ADMINISTRATIVE MESSAGES

A. All messages sent on the TIME System must deal with authorized law enforcement related matters.

B. Prohibited administrative messages as outlined in the TIME Operator's Manual will not be sent by terminal operators.

C. All-point messages must be sent from TSCC and be in accordance with the regulations as described in the TIME Operator's Manual.

D. Area broadcast messages will only be sent in accordance with the procedures set forth in the TIME Operator's Manual. Area broadcast messages should not be sent in lieu of a record entry (wanted or stolen).

E. NLETS regional messages must meet the same criteria as an administrative message. Each NLETS region includes the FBI NCIC Control Center in Washington, D.C. It is not necessary to receive approval from TSCC to initiate NLETS regional broadcast messages.

XI. TIME SYSTEM SECURITY PROCEDURES

A. Security Management – The Department will appoint an individual as the agency's Local Security Officer. The Local Security Officer will be responsible for maintaining and monitoring all security aspects of the Department's access to the TIME System.

B. Physical Security — The physical security for Time System terminals shall conform to procedures set forth in Version 5.0 of the Criminal Justice Information Services Security Policy, which is outlined in the Department's TIME System Security Manual.

C. Access--The Local Security Officer shall manage information system accounts used to access the TIME System. The Local Security Officer's responsibilities include but are not limited to: establishing, activating, modifying, reviewing, disabling, and removing these accounts.

Access to various functions of the system shall be controlled by privileges assigned to individual users by the Local Security Officer. Access to privileged functions and security (relevant information) shall be restricted to explicitly authorized personnel. The most restrictive rights/privileges needed by users for the performance of their specified tasks will be enforced to limit access to the TIME System to only authorized personnel with the need and right to know.

The Local Security Officer will assign an initial log-in password to certified new users to the information system. Once logged on, new users will be required to change their password which will conform to procedures set forth in Version 5.0 of the Criminal Justice Information Services Security Policy, which are outlined in the Department's TIME System Security Manual.

D. Media Protection--Electronic and Physical media shall be stored within physically secure locations with access restricted to authorized individuals. Electronic media containing TIME System information shall only transported outside the secure locations by authorized personnel with activities restricted solely for purposes associated with the transportation. All media will be sanitized or degaussed prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media and physical media shall be destroyed. Sanitation and Destruction of media shall be witnessed or carried out by authorized personnel.

Michael Meeusen
Chief of Police

This Policy & Procedure cancels and supersedes any and all written directives relative to the subject matter contained herein.

Initial 06/01/2015