KENOSHA POLICE DEPARTMENT

POLICY AND PROCEDURE

81.2 Network Security and TIME System Access

Effective Date:	10/16/2018	**Revision Date:**	10/16/2018
Action:	Wisconsin Department of Justice Agency Agreement	**Number of pages:**	2

I. PURPOSE

The purpose of this policy is to ensure appropriate use of the Department of Justice TIME and e-TIME systems. The TIME system provides access to driver and vehicle information, criminal history and warrant inquiries along with other restricted material. The e-TIME system provides access to the TIME system through the internet.

II. POLICY

It is the policy of the Kenosha Police Department that access to the TIME system directly and through e-TIME is limited to trained personnel and only for official Kenosha Police Department business.

III. TIME and e-TIME SYSTEM ACCESS

A. The Wisconsin Department of Justice maintains the TIME and e-TIME systems therefore access to the system is ultimately under their control.

B. Access to e-TIME is limited to employees who have been authorized by the TIME Agency Coordinator and designated by the Chief of Police. No employee will use the login name and password of another to access the system.

C. Access to e-TIME is only permitted from department computers unless otherwise specified and authorized in writing; access from an unauthorized computer is prohibited.

D. Only persons who obtain and maintain the D.O.J. required training will be granted access to the TIME system whether directly or through e-TIME.

E. The department shall maintain a record of employees who have been granted permission to use the TIME or e-TIME Systems. Employees who are no longer authorized to access either TIME or e-TIME will be removed from the list maintained by the Department of Justice.

F. Any employee receiving a request for information obtained through the TIME system shall ensure that the person making the request is authorized to receive such information before providing it.

G. The TIME and e-TIME systems are only to be used for official Kenosha Police Department business.

H. All TIME system information received in printed form will be destroyed when it is no longer needed.

I. Use of the TIME system directly or through e-TIME will be monitored and any misuse of the system or unauthorized disclosure of information obtained through the system will result in discipline.

J. Computers that have been used for TIME / e-TIME access shall have the hard drive destroyed when removed from inventory.

IV. LOCAL AGENCY SECURITY OFFICER (LASO)

A. The Chief of Police will appoint a LASO for the Department. The LASO is responsible for ensuring that the agency complies with both the CJIS Security Policy and this policy.

B. The tasks assigned to the LASO include but are not limited to:
   1. Monitor the creation and conduct regular audits of Department system account, including but not limited to Microsoft Active Directory, Microsoft Exchange, TIME System, e-TIME, and any other third party software that may allow access to NCIC, TIME or other Criminal Justice Information (CJI). The LASO shall ensure that system accounts are deactivated as soon as practical after department employment has ended or other disqualifying events have occurred.
   2. Conduct a weekly review of system audit logs for inappropriate, unusual or suspicious activity. Additionally, the LASO shall coordinate with Kenosha Joint Services to review third party software logs for inappropriate, unusual or suspicious activity.
   3. Ensure that personnel security screening procedures are being followed as stated in CJIS Security Policy in coordination with the departments TIME System Agency Coordinator (TAC).
   4. Ensure that approved and appropriate security measures and incident response handling procedures are in place and working as expected.

V. INFORMATION SECURITY INCIDENT RESPONSE

A. The Kenosha Police Department shall take steps to protect Criminal Justice Information (CJI) in both physical and logical environments. To ensure the security of CJI, the Department shall establish operational procedures to detect, analyze, contain and recover data from network security events.

B. All employees, contractors or third parties with access to the Departments network will be made aware of procedures for reporting network security events. If a network security event is detected, employees will report all such events to the Department LASO. Security events include but are not limited to the loss or theft of media or equipment containing CJI, suspicious or malicious software in the Departments network environment or other unusual network activity.

C. The Department LASO will track, document and report network security events to appropriate officials, including reporting events in writing to the FBI CJIS Information Security Officer using forms provided in the FBI CJIS Security Policy. Where feasible, the Department will employ automated mechanisms to assist in the detection and reporting of network security events.