MILWAUKEE POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

680 – COMPUTER EQUIPMENT, APPLICATIONS and SYSTEMS

GENERAL ORDER: 2022-XX **ISSUED:** April 7, 2022	**EFFECTIVE:** April 7, 2022	**REVIEWED/APPROVED BY:** Assistant Chief Nicole Waldner **DATE:** February 25, 2022
ACTION: Amends General Order 2021-03 (March 26, 2021)		**WILEAG STANDARD(S): 6.4.1, 10.1.1, 10.1.11**

680.00 PURPOSE

This standard operating procedure is intended to provide guidelines for the use of computer equipment within the department and to set guidelines for the use of various applications. This includes personally owned computers that are used in department activities.

680.05 COMPUTER GUIDELINES

A. Computer resources are provided for department business, however, users are authorized limited incidental use of the department's resources for personal purposes per 680.45.

B. Only software purchased, developed or otherwise obtained by the department is to be used on department equipment.

C. No additional computer hardware and/or computer peripheral equipment shall be installed, moved, removed, or reallocated without the written approval of the Information Technology Division. All hardware and peripheral equipment installations, moves, removals or re-allocations are the responsibility of the Information Technology Division.

D. Additional computer hardware, software applications and/or processes for new departmental projects shall not be acquired through city purchasing, asset forfeiture, grants, donations, etc. without first notifying the Information Technology Division for planning and scheduling. It is the responsibility of the Information Technology Division to ensure that additional computer hardware, software applications and/or processes are compatible and/or compliant with current MPD policies, DPW MOU infrastructure, city network policies, state CIB and federal CJIS security guidelines.

E. Computers and all associated peripherals, software, documentation and data, including instruction manuals, are not to be moved from their authorized location without the prior consent of the Information Technology Division.

F. Any program or work product developed on department equipment or on department time is the property of the city of Milwaukee and shall not be sold or given away without proper authorization.

G. In accordance with the purchase of hardware and software by the city of Milwaukee,

the city is subject to the provisions of the copyright laws. As a practical matter, these laws prohibit the copying of computer software for other than archival and backup purposes.

H. In compliance with city of Milwaukee computer policy, the Information Technology Division will only support software meeting their software standards. Other authorized software running on department computers must have the master disks, manuals and registration information next to the computer. If registration information cannot be supplied, the software must be removed immediately.

I. If shareware or public domain software is operating on a department system, the documentation requirements established above must be maintained. In addition, a *Department Memorandum* (form PM-9E) shall be submitted to the Information Technology Division for purposes of identifying ownership.

J. Periodic audits and preventative maintenance programs will be performed by the Information Technology Division. These procedures will ensure that only authorized software is operating on all department systems and that the equipment is operating effectively and efficiently according to the purpose for which the equipment was acquired.

680.10 TIME AND eTIME SYSTEMS (WILEAG 6.4.1, 10.1.1, 10.1.11)

The Transaction Information for the Management of Enforcement (TIME) system and eTIME (the web based application of the TIME system) provides a central system for the collection and dissemination of information of mutual concern to law enforcement agencies. It is an efficient and expeditious means by which the procurement, exchange and transmission of information with law enforcement agencies state and nationwide is accomplished. The system also provides an effective method of administrative communication for law enforcement purposes. The TIME and eTIME systems are interfaced with numerous local, state and national agencies, departments and files. It is of vital importance that regulations pertaining to its use be complied with to ensure individual rights are not violated and to minimize issues of liability. Data service agencies have agreed to make information available to law enforcement and criminal justice over the TIME, eTIME and NCIC systems for the specific purpose of facilitating the administration of criminal justice. Any misuse of this information or violations of these understandings jeopardizes the availability of information for all participating agencies. The systems and the information contained therein must be protected from possible physical, natural and hardware vulnerabilities.

A. TIME AGENCY COORDINATOR

The TIME agency coordinator (TAC) is responsible for coordinating training of the functions of the terminal, ensuring compliance with NCIC and Crime Information Bureau (CIB) policy and regulations including validation and other requirements, and formatting training in conjunction with CIB certification, re-certification and specialized training classes. The TAC will ensure a proper number of Training Resources Available on the InterNet (TRAIN) administrators are assigned to work locations/shifts that utilize the TIME system. The TAC will attend CIB TIME system TAC training

within one year of appointment as the department's TAC.

B. TRAIN ADMINISTRATORS

Each work location which utilizes the TIME system will be assigned at least one TRAIN administrator. The TRAIN administrators will assist the TAC to ensure all members at the work location requiring TIME certification are properly trained and re-certified.

C. CERTIFICATION OF TIME AND ETIME SYSTEM USERS

1. Only those members who obtain and maintain the required Department of Justice (DOJ) training will be granted access to the TIME and eTIME systems. Members using the TIME and eTIME system may only use the system for purposes for which they were certified.

2. All members of the department who use Criminal Justice Information Systems (CJIS) or who routinely review criminal justice data as a position responsibility will be required to be re-certified every two (2) years. Re-certification notifications and administration will be handled by the department's TAC.

D. DATA PROTECTION AND SECURITY

Data security is of the utmost concern and to ensure the security of sensitive law enforcement data the following guidelines will be employed:

1. All members of the department who have authorized access to FBI CJIS systems and those who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS systems will have state and national criminal history record checks by fingerprint identification. These checks must be conducted within 30 days upon initial employment or upon assignment to areas within the police department that conduct criminal justice information transactions. Police members who have been fingerprinted and certified by the Wisconsin Law Enforcement Standards Board (LESB) already meet this requirement.

2. Each member of the department having TIME and/or eTIME system privileges has been issued a unique system login. Members are required to log out or lock all Criminal Justice Information Systems from unauthorized access when the member is not present at the system.

3. All transactions from criminal justice data systems are considered confidential and may not be released to non-law enforcement agencies or personnel.

4. Any individual authorized to use the TIME or eTIME system who receives a request for criminal justice information from another individual must ensure the person requesting the information is authorized to receive the data. Each data service has its own rules for secondary dissemination of records, which may include requirements for logging, identification of the purpose of the request and identification of the specific individual receiving the record. Most records may be legitimately

disseminated to another criminal justice employee/agency when the purpose of the request is criminal justice related.

5. The printing and/or copying of criminal justice data will be limited to the time of need and reproductions limited to the smallest quantity to complete the job.

E. SECURITY OF SENSITIVE LAW ENFORCEMENT INFORMATION

1. Any device (e.g., computer monitors, smart phone displays) that displays criminal justice information will be positioned in such a way as to prevent unauthorized individuals from accessing or viewing the criminal justice information.

2. Non-department members without a department-issued white ID card, requiring access to any non-public area of a police facility that conducts Criminal Justice Information System transactions must be entered into the Sharepoint electronic Visitors Log and be issued an orange visitor ID card prior to admittance into an area not normally designated as publicly accessible. See SOP 780 Police Facilities Security for full information on visitors to police facilities.

3. Electronic and physical media containing sensitive criminal justice information will be physically stored in a secure or controlled area to prevent unauthorized access or viewing.

4. When electronic or physical media containing sensitive law enforcement media is being transported or disposed of outside of a controlled area, the transporting and/or disposal shall be observed or completed by CJIS cleared personnel.

5. Electronic, printed or other media containing criminal justice information will be securely disposed of when no longer needed or required. Printed media will be destroyed by shredding or by placing the media in secure shredding containers for later shredding. Electronic media will be sanitized, wiped or degaussed prior to disposal.

F. PROPERTY FILES (TIME SYSTEM)

1. Stolen property may be entered into TIME system if the owner or custodian of the property has made a theft report that is on file.
(WILEAG 10.1.11.1)

2. Stolen Property File Entries with Special Requirements

a. Stolen / Rented / Leased / Vehicles

A loaned, rented, or leased vehicle or boat that has not been returned may not be entered unless an official police theft report is made of a files complaint results in the issuance of a warrant charging embezzlement, theft, etc. See SOP 630 Vehicle Thefts, Prior Authority Vehicle Use, and Theft by Fraud regarding.

b. Felony Vehicles

A vehicle used in the commission of a felony/wanted in connection with a felony may be entered immediately providing the whereabouts of the vehicle is unknown. A vehicle does not have to be reported stolen to be listed as a felony vehicle.

c. Stolen / Missing License Plates

A stolen or missing license plates may be entered into the CIB/NCIC database. If only one license plate was taken, the plate may only be entered when the remaining plate is removed/destroyed and the complainant/owner obtains new/corrective registration. If the owner/complainant wishes to retain the same license plate number, no entry can be made to the database. Documentation in the Record Management System (RMS) must be maintained detailing what happened to the remaining plate, and the fact that the owner was directed to obtain corrective registration.

d. Recovered Firearms

A firearm that has been recovered by a department member must be queried through the TIME system to determine if the firearm was listed as stolen. If the firearm was not listed as stolen, the firearm shall be entered as a recovered firearm provided it remains in the custody of the department.

e. National Insurance Crime Bureau (NICB)

The National Insurance Crime Bureau maintains a database of vehicle records. This database includes information about manufacturer's shipping and assembly, vehicles imported and exported, thefts, impounds, salvage, auction, pre-inspection, vehicle claim, lien and rental information. In addition to providing access to these files, TIME System users may list vehicles on the NICB impound file. All NICB entries and queries are based upon a vehicle identification number. Prior to making entries to the NICB impound files, the department must have the vehicle in question in its possession or control.

f. Caution Indicator

When an agency lists property in the CIB/NCIC databases, they may have the option of having their entry bear a notation of 'CAUTION.' This notation should be listed on an entry whenever this agency has information that the subjects in a stolen vehicle/boat are armed and dangerous, or when an agency wishes a recovered stolen item be held for latent fingerprint examination. This determination should be made after an examination of all supporting documentation in the incident reports, to include past dealings with subject and/or suspect, and information listed on criminal history or other files. The reason for the armed and dangerous caution indicator must be included in the Remarks Field.
(WILEAG 10.1.11.1)

3. Accuracy of Records

   The accuracy of records is an integral part of the TIME system and all entries of stolen property shall be in accordance with TIME system requirements. The member entering the record into the TIME system shall include assuring all available cross-checking was made and that the data in the record matches the data in the incident report or applicable request to enter stolen property into the TIME system.
   (WILEAG 10.1.11.1, 10.1.11.2)

4. Property Data Files Modification / Supplementation

   Department members shall enter as much information about the stolen property as is available, and if data becomes available to a later date, the record shall be modified or supplemented to include the new information. Inquires should be made to the TIME System DOT files, CHRI files, Department of Natural Resources files, etc., RMS, and any other existing records to obtain all the data available. Any new information should be included in a supplemental report to show where the identifiers/new information was obtained. Any information that cannot be verified shall not be included in the data entry.
   (WILEAG 10.1.11.2)

5. Property Data File Cancellations

   All entries shall be removed as soon as it is learned that the property has been recovered. It is not permissible to wait until property is in the department's possession. The entry must be cancelled as soon as practicable. Once a record has been cancelled, documentation of the cancellation and reason for cancellation will be retained in the case file. The record should be queried again to ensure that it has indeed been removed from the database.
   (WILEAG 10.1.11.3)

6. Purged Property Records

   Records entered to the CIB/NCIC databases are retained in these files for a specified period of time in accordance with TIME system guidelines. When the specified time period has passed, records are purged from the databases. When notice is received a record has been removed from the database, a supplemental report will be filed to reflect this information. These records will not normally be re-entered unless there is some investigative value to re-entering the item to extend the retention period. This determination will be made on a case by case basis by a supervisor.

7. Department members shall have 24-hour access to the department's stolen property files through RMS.
   (WILEAG 10.1.11.4)

G. Members who violate the TIME system policy may be subject to disciplinary action.

680.15 LAW ENFORCEMENT NATIONAL DATA EXCHANGE (N-DEx)

A. The N-DEx system provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries.

B. Only sworn members who have successfully completed training provided by the Law Enforcement National Data Exchange may access the N-DEx system. Members are required to be re-trained on policy matters and data use rules for the N-DEx system on a biennial basis through the Law Enforcement National Data Exchange. Members who do not complete the initial training or fail to meet the subsequent biennial training requirement shall not access the N-DEx system.

C. Members shall submit training certificates provided by the Law Enforcement National Data Exchange upon successful completion of required training to the department's N-DEx coordinator.

D. The department's N-DEx coordinator shall retain a copy of all N-DEx training certificates. The department's N-DEx coordinator shall ensure a copy of all training certificates are sent to the Training Division for inclusion in the member's training record.

680.20 DEPARTMENT EMAIL

A. Email is a vital means of communication between members of the department and for relaying important electronic correspondence. Electronic memorandums, directives or instructions issued by the department or a supervisor sent via email will be treated as having received a verbal directive from the department or supervisor.

B. All members are required to check their city of Milwaukee email account at least once during each tour of duty. To help facilitate access, the department email system can be accessed via the department intranet or the internet from a computer outside of the department.

1. Intranet Access

   To access the department email system from the intranet, go to the department's blue background home screen and click the "Email – MPD" link found in the "Favorite Links" column.

2. Internet Access

   To access the department email system from a computer with the internet, enter the following URL into the web browser: https://login.microsoftonline.com.

C. To "log-In" to an email account, it will require the members "user name" (usually, but not always, the member's first initial and first five (5) characters of the last name) and the member supplied password. Members are reminded to "log off" after each email session. For assistance with the department email system, call the Information Technology Division Help Desk at extension [redacted].

D. Email messages distributed outside the department shall be viewed as direct correspondence from the department. Email users are prohibited from representing the department, either implicitly or explicitly, unless authorized by a commanding officer to do so. Other specific email provisions and/or restrictions may apply and can be found in this SOP.

680.25 USE OF PERSONALLY-OWNED COMPUTERS

A. WRITTEN REQUEST

Members wishing to use personally owned computers for department business shall submit their request on a *Department Memorandum* (form PM-9E) to their commanding officer. This report shall describe the functions to be performed by the computer and the objectives to be achieved.

B. SPECIAL PERMISSION

Personally owned computers shall not be connected to any department telephone system or department network without the specific permission of the Information Technology Division.

C. COMMANDING OFFICER'S RESPONSIBILITY

1. Approve or deny requests by members to use personally owned computers for department business. This may be done only in cases where the computer is not connected to a department telephone or network system.

2. When connection to a department telephone or network system is required, the original request shall be forwarded to the Information Technology Division for review.

3. Copies of all requests, whether approved or denied, shall be maintained at the work location.

680.30 MEMBER'S RESPONSIBILITIES

A. All members shall check their city of Milwaukee email account at least once during their tour of duty.

B. Department members shall comply with the provisions of Milwaukee Police Department standard operating procedures regarding the confidentiality of department records, reports and information.

C. Computer input and output data shall be in compliance with the state of Wisconsin open records laws.

D. Additional care shall be exercised concerning sensitive department data. Sensitive data is defined as data that is not routinely available to the public. Under no circumstances is this information to be created, stored, processed or duplicated by

members outside of official department facilities without specific written permission of the member's commanding officer.

E. All passwords for software applications are to be treated as sensitive, confidential information and therefore shall not be shared with anyone including other department and non-department members. All passwords shall meet the minimum requirements of the applicable software application.

680.35 COMMANDING OFFICER'S RESPONSIBILITY

Commanding officers shall be responsible for:

A. Ensuring that all software used is legally acquired and installed.

B. Ensuring that access to sensitive data is limited to department members on a need–to–know and right–to–know basis.

C. Ensuring that user manuals are accessible to members using computers.

D. Ensuring that computer use at the work location is monitored and is in compliance with department guidelines.

680.40 USE OF DEPARTMENT-OWNED CELLULAR PHONES

A. Department issued cellular phones shall only be used for official police department business and only be used by department members unless exigent circumstances dictate otherwise. All cellular phone records are subject to public disclosure in accordance with Wisconsin Public Record Law (Wis. Stat. § 19.31-39).

B. Only members of the department authorized by the assistant chief or inspector of the Administration Bureau shall be issued a department-owned cellular phone.

C. Members issued department-owned cellular phones shall have no expectation of privacy with regard to any communication made with or stored in their issued cellular phone.

D. Requests for a department issued cellular phone shall be made in writing on a *Department Memorandum* (form PM-9E) and submitted through the chain of command for approval.

E. Commanding officers issued department-owned cellular phones for their work location shall ensure:

1. Proper use, care, and maintenance of each cellular phone.

2. Each cellular phone is properly secured and stored when not in use (if not assigned to a specific member).

3. The Technical Communications Division (TCD) Telecom supervisor is notified of

any damaged or missing cellular phone equipment.

4. Only authorized members are provided a department-issued cellular phone.

5. Ensure the cellular phone and associated equipment is returned to the TCD Telecom supervisor if a cellular phone is no longer required for an assigned member's position or upon resignation or retirement from the department.

F. Department members issued department-owned cellular phones shall:

1. Ensure proper use, care, and maintenance of the cellular phone.

2. Ensure inappropriate or unprofessional messages are not sent from the cellular phone. Members shall ensure that inappropriate or unprofessional content is not accessed on the internet via department-owned cellular phones.

3. Ensure that a professional generic voice mail greeting and ring tone is developed and used for each assigned cellular phone.

4. Check for voice mail messages on a daily basis to ensure that any outstanding messages are returned in a timely manner.

5. Immediately report damaged or missing cellular phone equipment to their supervisor and the TCD Telecom supervisor.

6. Ensure the cellular phone and associated equipment is returned to the member's commanding officer if a cellular phone is no longer required for the member's position or upon resignation or retirement from the department.

G. The TCD Telecom supervisor shall:

1. Be responsible for issuing and establishing an audit log of all department issued cellular phones and associated equipment.

2. Be responsible for reviewing all monthly cellular phone invoices, including the detailed billing records, for accuracy and to ensure each cellular phone is billed on the correct service plan.

3. Prescreen monthly billing records for any cellular phones with questionable charges and forward the detailed billing records for these cellular telephones to the Administration Bureau assistant chief for review.

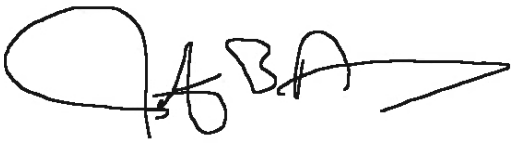
4. In conjunction with the Inspections Section, conduct an annual audit of cellular phones and associated equipment assigned to each bureau to ensure there is a continued need for each assigned cellular phone and to ensure each cellular phone is assigned to the appropriate member.

680.45 ELECTRONIC COMMUNICATION - RIGHT TO PRIVACY

The content of all electronic communication, including but not limited to electronic mail (e-mail), e-mail attachments, instant messaging, text messaging, voice over internet protocol (VOIP), Twitter, Facebook and other 'electronic social media,' YouTube, records of internet use (including web sites accessed) and all other means of electronic communication (hereinafter "electronic communication") sent, received, or accessed through the department's computer network, CAD system (by MDC or other terminal), department cellular telephones, and other electronic communication devices provided by the department are considered the property of the department. This includes all electronic communication sent, received, or accessed from personal accounts (e.g., Yahoo, G-mail) on department equipment.

As such, the Information Technology Division has the right to monitor, review, audit, and otherwise access the content of all electronic communication sent, received, or accessed on department equipment with or without prior notice to the member for both non-investigatory work-related reasons, and for investigation of member misconduct. Members have no expectation of privacy or confidentiality in electronic communication sent, received, or accessed on department equipment. Electronic communication is subject to state record retention requirements and may be subject to the Wisconsin public records law. The content of employee electronic communication may be subject to disclosure in litigation, audits, and other purposes. Users are authorized limited incidental use of the department's resources for personal purposes, but members have no expectation of privacy or confidentiality in such use. Members are strongly encouraged to use their own communication devices for personal and confidential communications.

Members are prohibited from sending, receiving, or accessing electronic communication that is insulting, profane, vulgar, lewd, indecent, sexually explicit, illegal, profit-making, political, unprofessional, or in violation of the department's policies, including but not limited to its EEO policies.



JEFFREY B. NORMAN
CHIEF OF POLICE

JBN:mfk