MILWAUKEE POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

680 – COMPUTER EQUIPMENT, APPLICATIONS and SYSTEMS

GENERAL ORDER: 2024-11 **ISSUED:** February 26, 2024	**EFFECTIVE:** February 26, 2024	**REVIEWED/APPROVED BY:** Assistant Chief Nicole Waldner **DATE:** January 8, 2024
ACTION: Amends General Order 2022-20 (June 13, 2022)		**WILEAG STANDARD(S): 6.4.1, 10.1.1, 10.1.11**

ROLL CALL VERSION
Contains only changes to current policy.
For complete version of SOP, see SharePoint.

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~~80.

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~~ Asset management 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.

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 and acquiring new hardware, software, and computer-related equipment.

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. The Information System Coordinator (ISC) program allows authorized liaisons to conduct periodic IT-equipment audits under the direction of the police information systems director and information systems manager.

680.10 INFORMATION TECHNOLOGY DIVISION REQUESTS

A. Requests from all department work locations to the Information Technology Division for any hardware, software, project needs, or services that have a fiscal impact, regardless of dollar amount, shall be forwarded by the respective work location’s commanding officer on a *Department Memorandum* (PM-9E) through the chain-of-command to the requesting member's inspector of police.

B. A recommendation from the commanding officer is required with all such submissions. The commanding officer's recommendation is to include a brief notation indicating why approval is necessary. Any requests submitted without a commanding officer's notation of recommendation will be returned to requesting work location.

C. The respective bureau inspector will review each request and forward the request to the inspector of the Administration Bureau with a recommendation.

D. The inspector of the Administration Bureau, in conjunction with the police information systems director, will review the request and make a final decision.

E. Any projects that are approved for asset forfeiture funds but are related to the Information Technology Division shall follow the same approval process outlined in subsections A-D to ensure no additional costs or staff hours are incurred by the department for the project without prior approval. The Information Technology Division will work in conjunction with the Budget and Finance Division to ensure proper accounting of all funds related to the project, if approved by the inspector of the Administration Bureau and the police information systems director.

680.15 MPD NETWORK

A. The network manager maintains subnets, access points, wireless local access network (WLAN), virtual LAN (VLAN), servers, and any devices on the network wireless network. All hardware and software utilized by department work locations must adhere to IT security protocols. Changes to production software, equipment, and/or network functionality must go through the IT change management process.

B. The network manager and information systems manager, under the direction of the police information systems director, create a consolidated group of related department units that have the management authority and responsibility for compliance with IT policies, standards, and guidelines. Installation of all network devices must be approved and coordinated by the network manager. This includes, but is not limited to, routers, switches, remote access devices, Internet of Things (IoT) devices, modems, wireless access points, or any other device that allows access to the MPD network.

680.20 APPLICATIONS

A. All applications installed on MPD computer equipment connected to the MPD network are the sole responsibility of the Information Technology Division and must be approved by the police information systems director and data services manager. New software requests must be submitted through the chain of command on a *Department Memorandum* (form PM-9E) and approved prior to installation. This also includes division and department-specific specialty software programs and applications.

B. Downloading freeware applications on MPD equipment is prohibited without an approved *Department Memorandum*. For additional computer usage guidelines, see SOP 680.05 Computer Guidelines.

C. The Information Technology Division supports the Police to Citizen (P2C) online reporting website, but the application is the responsibility of the Records Management Division.

680.25 SECURITY

A. MPD network security systems and safeguards must not be bypassed. Encryption key management control and user system access is the responsibility of the Information Technology Division. Access to assets, both physical and logical, is limited to authorized users, processes, and devices and is managed by the systems security administrator. This includes defining and monitoring administrator tasks involved with protection, storage, organization, access controls, and lifecycle management of encryption keys.

B. Identification Cards

1. Department members shall use their identification card access badge to gain entry to an MPD facility or parking garage. Members shall not share identification card access badges.

2. Lost or stolen identification card access badges shall be reported to the MPD Help Desk as soon as possible and reported lost or stolen to a supervisor in accordance with SOP 340 Uniforms, Equipment, and Appearance.

680.30 HELP DESK SUPPORT

A. The MPD Help Desk manages and supports all devices, equipment, and connectivity on the network. The MPD Help Desk collaborates with the Information System Coordinators (ISCs) to ensure district, divisions, and bureaus have the required systems and capabilities. The ISCs help ensure the equipment is operational and in compliance with MPD IT security, policies, and procedures by communicating and working with the Help Desk staff members.

B. The Information Technology Division manages assets and inventory through periodic audits. MPD assets and equipment are assigned to a position and/or rank, not to an individual. New software and hardware requests must be approved by submitting a request through the chain of command on a *Department Memorandum* (form PM-9E) prior to installation.

680.35 FIELD TECHNOLOGY UNIT (FTU)

A. The FTU manages mobile data computers (MDCs), connectivity, and other MPD squad and motorcycle communication and video equipment and devices. Installation of security patches and MDC updates are also performed by the FTU. Further, AXON support for body worn cameras and Evidence.com including configuration, commissioning, and troubleshooting is performed by the FTU Division.

B. RADIO COMMUNICATIONS

The Information Technology Division is responsible for radio system communication. The communication systems manager maintains radio operations.

680.40 USER ACCOUNT CREATION, ACCESS, AND VALIDATION

A. New user accounts are created only upon written notification from:

1. MPD Human Resources Division (HR) - for permanent hire personnel, civilians or sworn.

2. MPD CJIS coordinator - for vendor or contract personnel.

B. MPD HR provides full user name, PeopleSoft number (PS#), title of position, work location and allows for the following:

1. User network account and J: drive creation.

2. User network N: drive permissions added based on position, rank and location.

3. User email account creation.

4. User physical access account creation with location clearances based on position added.

5. User Uniflow print services account creation.

6. User Record Management System (RMS) account created, all sworn automatically and as needed by position for civilians. Civilians require an authorizing email from supervisory personnel.

7. User Jail Management System (JMS) account creation, all sworn automatically and as needed by position for civilians. Civilians require an authorizing email from supervisory personnel.

C. MPD CJIS coordinator provides full name, vendor information, CJIS clearance approval and expiration date and CJIS approved network access and physical location access.

1. Network and physical access created only as specified in approved *Sponsorship Request for Non-Departmental Personnel* (form PL-8E).

2. Any additional changes requested require updated and approved PL-8E.

3. CJIS coordinator advises 90 days in advance of any expiring CJIS clearances for vendors and contractors.

4. Notification emails sent to vendor or contract personnel regarding upcoming CJIS

expiration and requirements to extend/renew clearance.

D. Promotion, Transfer or Personnel Orders provide official notification of MPD sworn and civilian departmental changes.

MPD Sworn and Civilian User accounts updated as stated per order.

E. MPD HR provides check out sheets via email for MPD personnel that will or have left the department.

1. Upon termination, network accounts are disabled and moved into the Disabled User Group in Active Directory.

2. Physical access disabled in CCURE.

3. Email account disabled and moved to Disabled Users in City ITMD email server.

4. All remaining accounts disabled/archived.

F. Upon notification from the Internal Affairs Division of disciplinary actions against MPD members, specified member access and all accounts disabled until adjudication notification from the Internal Affairs Division.

G. Any MPD member or contractor that temporarily needs access to a network N: drive folder or physical access location are required to provide an authorized *System Access Request* (PSAR-E form) or updated PL-8E respectively. The commanding officer of the work location in question must approve the form.

680.~~10~~45 TIME AND eTIME SYSTEMS (WILEAG 6.4.1, 10.1.1, 10.1.11)

H. Members requesting to add features to an eTIME account must send an email to a Milwaukee Police Department Time Agency Coordinator and cc the supervisor approving the request. Members shall not send email requests to the eTIME (State of Wisconsin) or contact eTIME by telephone.

680.~~15~~50 LAW ENFORCEMENT NATIONAL DATA EXCHANGE (N-DEx)

680.~~20~~55 DEPARTMENT EMAIL

680.~~25~~60 USE OF PERSONALLY-OWNED COMPUTERS

B. SPECIAL PERMISSION

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

680.~~30~~65 MEMBER’S RESPONSIBILITIES

680.~~35~~70 COMMANDING OFFICER'S RESPONSIBILITY

Commanding officers shall be responsible for:

C. Ensuring that user manuals are accessible to members using computers. ISCs assist commanding officers and the department by helping to verify compliance and IT-equipment locations and policies.

680.~~40~~75 USE OF DEPARTMENT-OWNED CELLULAR PHONES

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

3. The ~~Technical Communications Division (TCD) Telecom supervisor~~ City of Milwaukee Information Technology Management (ITMD) is notified of any damaged or missing cellular phone equipment.

5. Ensure the cellular phone and associated equipment is returned to ~~the TCD Telecom supervisor~~ ITMD 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:

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

~~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~~80 ELECTRONIC COMMUNICATION - RIGHT TO PRIVACY

JEFFREY B. NORMAN
CHIEF OF POLICE

JBN:mfk