MILWAUKEE POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

785 – SPONSORSHIP OF NON-DEPARTMENT MEMBERS

GENERAL ORDER: 2022-XX **ISSUED:** February 7, 2022	**EFFECTIVE:** February 7, 2022	**REVIEWED/APPROVED BY:** Assistant Chief Nicole Waldner **DATE:** January 7, 2022
ACTION: Amends General Order 2019-17 (May 15, 2019)		**WILEAG STANDARD(S): NONE**

785.00 PURPOSE

The purpose of this standard operating procedure is to establish a policy regarding the obligations and requirements for Milwaukee Police Department (MPD) members sponsoring individuals from outside of MPD to have unescorted access to department facilities, resources, and network systems.

785.05 POLICY

It is the policy of the MPD that personnel not employed by the MPD who wish to have unescorted access to department facilities, resources, and network systems must be sponsored by an MPD commanding officer or civilian manager. The sponsor will be the commanding officer or civilian manager of the division, district, and/or bureau the non-department employee will be assigned to closely work with. Only non-department members with a demonstrated requirement for extended, consistent and frequent facility and/or network system access will be sponsored by MPD members.

The sponsor and the applicant shall both abide by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Service (CJIS) Security Policy, as well as the policies and procedures of the MPD.

Note: The Milwaukee Police Department shall not assume individuals with law enforcement and/or criminal justice credentials can be immediately authorized and provided physical and/or remote access to MPD facilities, resources or network systems.

785.10 PROCEDURE

Only non-department members with a demonstrated requirement for regular unescorted facility, resources or unsupervised network system access should be sponsored by MPD members. If the non-department member will only need sporadic access, he/she shall not receive sponsorship. Rather, SOP 780 Police Facilities Security shall be adhered to and these non-department members shall sign in and out as a visitor, issued an orange visitor's identification card and continuously be escorted while in restricted areas of MPD facilities.

The MPD has a three-tier system to identify the type of access non-department members shall be granted for facility, resource, or network system access. The tier level access is

determined based on their assignment within the department. All non-department members must successfully pass a CJIS background check to be granted access to the following tier levels:

Tier Level 1

- Individuals may be granted access to Tier 1 Applications if a current Memorandum of Understanding (MOU) exists between the MPD and the individual's agency and is in compliance with SOP 200 Project Management. The MOU must specifically state the type of information that MPD will share, as well as the system requiring access to include information obtained through the Federal Bureau of Investigation's Criminal Justice Information Services and other law enforcement sensitive information. Non-department members may only be granted Tier 1 system access by the requesting commanding officer's or civilian manager's respective assistant chief.

  Tier 1 Applications include:

  1. Computer Aided Dispatch (CAD)
  2. Records Management System (RMS)
  3. Traffic and Criminal Software (TraCS)
  4. Administrative Investigations Management (AIM)
  5. Intellinetics / Intellivue
  6. Axon
  7. Nice
  8. Network Shared Folders

- If MPD does not have an MOU on file, the sponsor may request that the non-department member be granted access to the MPD RMS by detailing the justification for this access on the *Sponsorship Request for Non-Department Personnel Form* (PL-8E).

Tier Level 2

MPD basic network access (this includes the MPD intranet and any system that is available through the intranet that does not require special access or a separate log in) may be granted to non-department members based on the scope of their assignment. If access is approved, the non-department member will be provided a network user name and password. Non-department members may only be granted network access by the requesting commanding officer's or civilian manager's respective assistant chief.

Tier Level 3

Non-department members may be granted physical access to MPD facilities only by the requesting commanding officer's or civilian manager's respective assistant chief.

A. SPONSORSHIP OF NON-DEPARTMENT MEMBER APPLICATION PACKET

1. Sponsor

   The sponsor is to ensure that only non-department members with a demonstrated requirement for regular facility, resource or system access will be sponsored.

   a. A sponsor shall be a commanding officer or civilian manager from the division, district, and/or bureau the non-department employee will be assigned to work with during the course of their duties.

   b. The sponsor is accountable for the supervision of the non-department member.

   c. The sponsor may be subject to disciplinary action as a direct result of federal, state, and/or local law or policy violations by the non-department member.

   d. The CJIS Compliance Coordinator (CJISCC) shall be responsible for maintaining a log of whom is being sponsored, the white identification card number each non-department member is issued, and the expiration date of the identification card. The CJISCC shall ensure the sponsorship is renewed in a timely manner (renewal not to exceed two years / reapplication every five years) when needed.

   e. The commanding officer or civilian manager shall maintain a log of whom they are sponsoring, the identification card number each non-department member is issued, and the expiration date of that identification card.

   f. When a commanding officer and/or civilian manager separates from the MPD, the member replacing him/her shall assume the sponsorship of all non-department members sponsored by the separating commanding officer and/or civilian manager. The commanding officer and/or civilian manager separating must brief his/her replacement regarding the responsibilities of sponsorship and pass on the log of all non-department members. If the separating commanding officer and/or civilian manager departs prior to a successor being appointed, the CJISCC shall inform the incoming commanding officer and/or civilian manager of his/her predecessor's sponsorships.

2. When a commanding officer and/or civilian manager identifies a person whom they wish to sponsor, they shall compile a Sponsorship of Non-Department Member Application Packet which shall include:

   a. *Sponsorship Request for Non-Departmental Personnel Form* (PL-8E);

   b. The completed last page of the TIME System Security Awareness Handout;

   c. The completed last page of the FBI Security Addendum; and

   d. A legible copy of the applicant's identification card.

3. Sponsorship Request for Non-Department Personnel Form (PL-8E)

   The non-department member will complete the grey personal information fields. The commanding officer and/or civilian manager will complete the remainder of the PL-8E. The commanding officer and/or civilian manager shall indicate exactly what facilities, network systems and resources they wish the non-department member to have access to. The commanding officer and/or civilian manager must provide detailed justification as to why each facility, network system, and resource has been requested. All requests for a non-department member to have access to any MPD facility, network system, or resource must be approved by the requesting commanding officer's or civilian manager's respective assistant chief.

   Note: All signatures on the PL-8E must be original. No facsimile signatures will be accepted.

4. State of Wisconsin Transaction Information Management of Enforcement (TIME) System Security Awareness Handout / FBI Security Addendum

   The non-department member shall review the TIME System Security Awareness Handout and FBI Security Addendum. After the handout has been reviewed, the non-department member will complete the last page indicating that he/she understands and will comply with the policy established by the handout. This includes, but is not limited to, the acquisition, use, and dissemination of information obtained through CJIS. Misuse of the TIME System or information obtained from it may be a violation of state and/or federal laws, and violations may subject individuals and agencies to criminal prosecution and/or other penalties. The unauthorized request, receipt, or release of TIME/National Crime Information Center (NCIC) System information can result in criminal/civil proceedings.

   Note: All signatures on the TIME Awareness/FBI Security Addendum must be original. No facsimile signatures will be accepted.

5. Legible Copy of the Applicant's Identification Card

   A legible copy of the applicant's identification card must be submitted. The identification must have a photograph of the applicant as well as the applicant's date of birth prominently displayed. This must be a valid state issued operator's license or identification card, city of Milwaukee municipal identification card, a United States passport, or federal government issued picture identification card.

B. The sponsor shall forward the completed application packet to the MPD CJISCC for processing. The commanding officer and/or civilian manager shall instruct the applicant to report to the Forensics Division – Criminal Records / Applicant Section to be fingerprinted. The applicant will inform the fingerprint technician that the fingerprints are for a "CJIS background check." The applicant must present valid photo identification card at the time the fingerprints are submitted.

C. If it is impractical for the non-department member to be fingerprinted by the Forensics

Division – Criminal Records / Applicant Section, the non-department member may be fingerprinted by his/her local law enforcement agency. Prints not directly obtained by MPD must be submitted on the standard FBI Fingerprint Card Form (FD-258). The "Reason Fingerprinted" field of form FD-258 should indicate that the fingerprints are for a "CJIS Background Check." The fingerprint card shall be forwarded to the Forensics Division – Criminal Records / Applicant Section for processing.

D. The Forensics Division – Criminal Records / Applicant Section shall check the fingerprints against MPD files for any criminal history record information. The fingerprints shall be forwarded to the State of Wisconsin and to the FBI's Integrated Automated Fingerprint Identification System (AFIS) for additional information. This process will take a minimum of fourteen days, therefore, the applicants fingerprints should be submitted as soon as possible. Once all of the results have been returned to the Forensics Division – Criminal Records / Applicant Section, the date and results will be documented in the Outside Jurisdiction Roster under the Applicant Fingerprint Data tab.

E. When sponsoring sworn members of other law enforcement agencies, the commanding officer and/or civilian manager may submit a letter from the non-department member's supervisor on their agency letterhead verifying that the non-department member has been vetted by their agency in lieu of having them submit their fingerprints to the Forensics Division – Criminal Records / Applicant Section. The letter must state that the non-department member has passed a national fingerprint based record check. The letter must list the specific name(s) of the individual(s) being sponsored.

F. The CJISCC shall forward a copy of the PL-8E and a copy of the applicant's identification card to the Human Resources Background Investigation Unit, which shall conduct a background investigation on each CJIS applicant. Each background check shall be conducted through the FBI National Crime Information Center (NCIC). The investigator shall indicate on the PL-8E the date the check was performed. The investigator shall document whether the candidate passed or failed the NCIC records check. If the applicant fails the background check, documentation justifying the failure shall be attached to the PL-8E by the investigator. This paperwork shall then be forwarded to the CJISCC.

G. Once all elements of the background check have been completed, the CJISCC shall notify the commanding officer and/or civilian manager of the results. If the applicant passes the background check, the CJISCC shall notify the Forensics Division – Forensic Imaging Lab that the applicant has been cleared to receive a white MPD identification card. If the applicant successfully passes the background check, the sponsor shall notify the applicant to proceed to the Forensics Division – Forensic Imaging Lab to receive his/her white identification card. The CJISCC shall ensure that all requirements are met before non-department members are granted access to facilities, network systems and resources controlled by the Milwaukee Police Department. The applicant must present a valid photo identification card to obtain his/her MPD identification card. The Forensics Division – Forensic Imaging Lab shall confirm that any individual requesting an MPD white identification card has been properly vetted and is eligible to receive an MPD white identification card. The

Forensics Division – Forensic Imaging Lab is responsible for photographing non-department members who have been vetted. Once the non-department member has been photographed, the Forensics Division – Forensic Imaging Lab shall create and issue the white identification card to the vetted non-department member. The original PL-8E shall be retained by the CJISCC for a period of seven (7) years.

Note: MPD will not grant access to any applicants who do not have a completed PL-8E form on record or who do not successfully pass the CJIS background check.

H. When a member of the Forensics Division – Forensic Imaging Lab issues an MPD white identification card, he/she shall notify the CJISCC. He/she shall also notify the MPD Systems Security Administrator (SSA), or designee. The SSA shall then ensure that all approved accesses are activated. When access is no longer needed, the SSA shall immediately deactivate the white identification card. The SSA, or designee, shall oversee that white identification cards and network accounts are activated and deactivated as necessary. While the white identification card is activated, the SSA, or designee, shall ensure that only access to the approved MPD facilities, resources, and network systems are granted. The CJISCC shall retain all PL-8E forms with original signatures.

I. By accepting the official MPD white identification card, the non-department member agrees to access MPD facilities, network systems and resources only in his/her official and on duty capacity. The non-department member shall not access MPD facilities, network systems or resources in any unofficial or off duty capacity whatsoever.

J. The sponsorship of a non-department member may not exceed two years. After a sponsorship has expired, the sponsor may renew the sponsorship by having the non-department member read the TIME System Security Awareness Handout and complete the last page. Once the CJISCC has received the newly signed handout, he/she shall request that a Support Specialist - Senior from the Information Technology Division reactivate or extend the non-department member's access. On the fifth anniversary of the original sponsorship, the non-department member will be required to submit all new application paperwork along with a new set of fingerprints. In addition, a new background check shall be conducted.

K. DEACTIVATION OF WHITE MPD IDENTIFICATION CARDS AND/OR RESOURCES

When the non-department member no longer requires access to MPD facilities and resources, the sponsor is responsible for recovering the non-department member's white identification card. The sponsor shall also notify the CJISCC and MPD SSA. The white identification card must be forwarded to the MPD SSA, or designee, for disposal.

L. LOST OR STOLEN WHITE MPD IDENTIFICATION CARDS

If for any reason the white identification card becomes lost, stolen or cannot be recovered, the sponsor must immediately notify the MPD Help Desk to deactivate the card. The sponsor shall then notify the CJISCC and the MPD SSA, or designee as soon as possible. An MPD supervisor is responsible for creating a Lost Property

incident report in the Records Management System (RMS).

JEFFREY B. NORMAN
CHIEF OF POLICE

JBN:mfk

APPENDIX

PROCESS FOR SPONSORING NON-DEPARTMENT PERSONNEL

Only non-department members with a demonstrated requirement for regular unescorted facility or unsupervised system access should be sponsored by MPD members. If the non-department member will only need access sporadically, he/she should not be sponsored.

SPONSOR SHALL compile an application packet to be completed which must include:

- PL-8E
- Last page of the TIME System Security Awareness Handout
- Last page of the FBI Security Addendum
- Legible copy of the applicant's Identification Card.

- The signatures on all documents **must be original**, no scans or facsimiles will be accepted.
- The Sponsor must add applicant to their Sponsor Log.
  - MPD ID card number and the expiration date of the card shall be added once approved and obtained

- Send COMPLETED packet via inter office mail to the CJIS Compliance Coordinator (CJISCC) for processing.
- The sponsor will instruct the applicant to proceed to the Forensics Division to be fingerprinted.

- Applicant shall go to the Forensics Division to be fingerprinted.
  - Must present a current Identification Card when being fingerprinted.
  - Applicant must tell the fingerprint technician that he/she is being fingerprinted for CJIS background check.

The CJISCC will forward the applicant packet to the Human Resources Background Investigation Unit.

The Human Resources Background Investigator will conduct a background check of the applicant's name. The Background Investigator will enter his/her findings on the PL-8E. The Background Investigator will then return the applicant packet to the CJISCC.

The Forensics Division will forward the fingerprints to the State for identification confirmation.

The State will check the prints in their database and send the results back to the Forensics Division.

If the applicant passes the background checks, the CJISCC will notify the Forensics Division and the MPD Information Technology Division that the applicant may be issued an MPD ID Card and it may be activated according to PL-8E authorized areas. **All MPD Access must be approved by the sponsoring member's Assistant Chief.**

If the applicant fails any part of the background check, the applicant will not be issued an MPD ID Card.