PBP FORM 290 **PITTSBURGH BUREAU OF POLICE** *"...accountability, integrity and respect."*		**SUBJECT:** **JUSTICE NETWORK (JNET) POLICY**		**ORDER NUMBER:** **51-1**
		PLEAC STANDARD:		**PAGE 1 OF 4**
REVISED DATE: **6/17/2016**	**EFFECTIVE DATE:** **6/29/15**	**ANNUAL REVIEW DATE:** **JUNE**	**RESCINDS:** **ALL PREVIOUS**	**AMENDS:** **NONE**

1.0 PURPOSE/POLICY

1.1 The purpose of this General Order is to establish procedures and guidelines for compliance with The Commonwealth of Pennsylvania Justice Network (JNET) Policy and Procedures, as they apply to PSP CLEAN Administrative Regulations, The Criminal History Records and Information Act (CHRIA) and Bureau policies regarding information technology and computer policies.

1.2 This policy will also govern the access of JNET and PSP CLEAN from the Premier MDC (MDT).

2.0 JNET SPONSORS

2.1 The Pittsburgh Bureau of Police will establish a JNET Sponsor who will verify the identity of users requesting JNET access, and that their job description requires them to have access to the requested user role. The JNET Sponsor will have the responsibility to approve and track JNET User requests.

2.2 The JNET Sponsor will have responsibilities as defined by JNET policy and will provide appropriate information to the JNET Registrar.

3.0 JNET REGISTRARS

3.1 The Pittsburgh Bureau of Police will establish JNET Registrars who will be responsible for registering JNET Users.

3.2 The Registrars will have the responsibilities defined in the JNET policy, including but not limited to:

3.2.1 Completing JNET Registrar Training.
3.2.2 Maintaining JNET Sponsor agreements.
3.2.3 Acting as Agency contact with respect to user registration issues.
3.2.4 Reporting violations of JNET Policy to the JTAC (Terminal Agency Coordinator) Officer.
3.2.5 Maintaining user records and other JNET user files as required.
3.2.6 Forwarding Criminal History Access requests to the JTAC Officer.
3.2.7 Updating user's enrollment status to JNET office (for reasons of retirements, arrests, transfers, separations, etc.).

4.0 JTAC OFFICERS

4.1 The Pittsburgh Bureau of Police will establish a JTAC Officer who will be the contact concerning all criminal history information accessed by JNET users. The current list of approved JTAC Officer(s) will be maintained by the Computer Operations Division.

4.2 The JTAC Officer will have all of the responsibilities outlined in JNET Policy, including but not limited to:

4.2.1 Ensuring that employees requesting Criminal History (CH) access are either JNET/CLEAN or PSP CLEAN certified, and that the User's certification is current.
4.2.2 Providing assistance to the Metropolitan Terminal Agency Coordinator (MTAC) for audits and misuse investigations.
4.2.3 Completing and signing CH access requests.
4.2.4 Enforce, disseminate, and interpret PSP CLEAN and JNET policies and procedures.

4.2.5 JTACs will conduct investigations if they have evidence of *JNET Policies and Procedures Misuse* potential misuse; or if they receive a request from the Agency Sponsor, or the JNET Security Administrator. In instances where the misuse report originates from the JNET Office, the JNET Security Administrator will forward the information to the Registrar or JTAC and request that they investigate the matter

5.0 JNET TRAINERS

5.1 The Bureau of Police will establish JNET Trainers who will be responsible for training Criminal Justice Users on the JNET overview and JNET CLEAN policies as appropriate to their needs.

6.0 JNET USERS

6.1 Officers are required to obtain and maintain a current JNET/NCIC/PREMIER MDC (MDT) account and access to Criminal History checks throughout employment with the Pittsburgh Bureau of Police.

6.2 In order to obtain that account and access, officers are required to take and pass a JNET OVERVIEW EXAM, and the Initial NCIC Exam when completing their initial registration for a JNET account.

6.2.1 Officers will be required to take and pass a JNET/NCIC Recertification Exam every two years to maintain access to the PSP Clean Portal XL and PREMIER MDC (MDT).

6.2.2 Officers hired after 01/01/2014 are required to have a Live Scan Fingerprint examination, as required by State and Federal regulations, prior to being granted access to JNET Criminal History information.

6.3.3 Officers hired prior to 01/01/2014 whose fingerprints are not currently on file will have to have a Live Scan Fingerprint examination completed in order to maintain their CH access.

6.4 Officers assigned and authorized as JNET Criminal Justice Users and JNET Criminal History Users shall abide by all JNET policies relating to JNET security agreements, workstation security, password security and applicable departmental policies on information technology and computer security.

6.4.1 One Time Passcode (OTP) will be used in addition to your username and password.
6.4.2 Officers shall not divulge their passwords to anyone.
6.4.3 Officers shall use JNET for **OFFICIAL CRIMINAL JUSTICE PURPOSES** only.
6.4.4 Dissemination of CH information will be in strict compliance with JNET/CLEAN/PSP, Penn DOT Policy and CHRIA.
6.4.5 Criminal History Users will maintain all appropriate dissemination logs and they will be subject to review by the JTAC.
6.4.5.1 Each Criminal History User receiving a CHRI response shall record any secondary dissemination of that information to another criminal justice agency, or to anyone who is legally entitled to receive such information in compliance with the JNET Policy. Secondary dissemination logs are subject to random audit.
6.4.6 JNET Criminal History Users will maintain an individual dissemination log on PBP Form #542.10 – JNET Record Information Log. This log will keep a record of the viewing or printing of the following information:
6.4.6.1 Criminal History Information;
6.4.6.2 Penn DOT Driver's History;
6.4.6.3 Photographs accessed through the WebCPIN application to develop a photo array. (Only the pictures used in the photo array must be logged.)
6.4.7 Every duty location shall have access to a manual containing the JNET/CLEAN training module, CLEAN Administrative Regulations, the CLEAN CCHR Manual, CLEAN Terminal Equipment Operator Manual and NCIC/POF & CLEAN PFA File.

7.0 PROCEDURE FOR REQUESTING INFORMATION FROM ANOTHER JNET USER

7.1 An officer requesting information from a Criminal History User shall have a legitimate criminal justice purpose for requesting the information.

7.2 The Officer requesting Criminal History information or Penn DOT certified records <u>shall</u> keep copies of the request and the hard copy of the documents in a secure location. The documents should be shredded when no longer needed.

7.3 In the event an Officer does not have access to JNET/NCIC/CLEAN/or Penn DOT information, he/she may call the Zone Desk Officer or CRRU to have Warrant Office Officers assist with accessing that information.

7.4 The JNET User accessing Criminal History or Penn DOT information for another officer will complete a PBP Form #542.10 JNET Record Information Log for the information accessed, and will note the name and badge number of the officer for whom the information was accessed and the reason for the request.

8.0 <u>DISSEMINATION LOGS</u>

8.1 Each officer shall keep his/her own dissemination log (PBP Form #542.10 “JNET Record Information”).

8.2 At the end of each calendar month, the original log will be turned in at the officer’s duty location.

8.3 A copy may be made and kept in the officer’s performance file at the duty location for one (1) year.

8.4 The original log shall then be forwarded to the Office of Professional Standards 15 days after the report period ends, where it shall be filed by year, month and officer. The original logs will be kept on file for 2 years in the event of an audit.

8.5 If an officer does not access JNET Criminal History or Penn DOT information in any given month, they will not be required to complete a PBP Form #542.10 JNET Record Information Log for that month.

8.6 Zone Supervisors will maintain the “Supervisor’s Monthly JNET Report” – PBP Form #52-1 that indicates whether or not each officer accessed JNET Criminal History or Penn DOT information for that month.

8.7 A copy of the Supervisor’s Monthly JNET Report will be made and maintained at the duty location for one year.

8.8 The original of the Supervisor’s Monthly JNET Report shall then be forwarded to the office of Office of Professional Standards 15 days after the report period ends, where it shall be filed by year, month and officer. The original logs will be kept on file for 2 years in the event of an audit.

9.0 <u>SECURITY</u>

9.1 JNET Users are responsible for reading the JNET User Security Agreement and agree to abide by the requirement set forth in the agreement. All JNET Users understand that any violation of the agreement may result in the loss of their individual JNET/Internet account and they further understand that disciplinary action up to, and including termination may be taken if they fail to abide by the requirements of the agreement.

9.2 While it is possible to access JNET/CLEAN/Penn DOT information from various mobile devices, Officers are reminded that EVERY instance where JNET/CLEAN/Penn DOT information is accessed needs to be logged on the Dissemination Log (PBP Form #542.10).

9.3 Pursuant to State and Federal regulations, any and all information accessed through JNET/CLEAN will be destroyed immediately after they have served their authorized criminal justice purpose to avoid any unintended access to that information.

9.4 If any Police Bureau member, vendor, contractor, or other personnel who have un-escorted access to Bureau of Police Buildings, are charged with an M-2 or higher, their access to JNET/CLEAN <u>**and**</u> physical access to any Bureau of Police Buildings where data from CLEAN is accessed or stored, will be suspended until a final disposition has been reached.

9.5 Access to JNET can only be on an agency issued or managed device that is CJIS compliant.

10.0 <u>MIS-USE SANCTIONS</u>: The following are sanctions that can be issued by CLEAN for mis-use of its systems. These sanctions are <u>***separate***</u> from Pittsburgh Bureau of Police Discipline. The sanctions listed in this regulation; <u>do not</u> need to follow a progressive order.

1. **“Warning”** means a letter of warning will be mailed to the agency administrator and the individual. The letter will state the administrative procedure/policy violated and the fact that further violations could result in suspension or revocation of an individual’s access to CLEAN.

2. **“Probation”** means that a person will be placed in a probationary status for a period running from the date of imposition. Further violations occurring during the probationary period may result in automatic suspension or revocation of a person access without further action. A copy of the probationary letter is provided to the person agency administrator and the individual.

3. **“Suspended”** means that the person will not be permitted to have access CLEAN/CJIS information for a fixed period of time. A copy of the suspension letter will be mailed to the person agency administrator and the individual.

4. **“Revocation”** means a permanent restriction on any access to the CLEAN and CJIS systems and information, whether directly; indirectly or through a third party.

10.1 Officers can be charged civilly, criminally and administratively for mis-use of the CLEAN systems.

10.2 A Sanction of Suspended or Revocation will affect physical access to any area where CLEAN data is stored or accessed.

Approved By:

Thomas Stangrecki
Cameron McClay
Chief of Police
ACTING CHIEF