JNET User Agreement

This PA Justice Network (JNET) User Agreement (Agreement) is entered into by and between the Commonwealth of Pennsylvania and you ("User", also referred to as "You") and is effective on the date this Agreement is electronically accepted by you. Keep a copy of this Agreement for your records.

You understand and acknowledge that your access to the Pennsylvania Justice Network ("JNET") and the information or data ("the content") provided by its data providers is contingent on you agreeing to and complying with the terms and conditions of this Agreement, which shall be sufficient consideration to enforce this Agreement. By electronically accepting this Agreement, the User agrees to conduct this transaction by electronic means and agrees to abide by the terms and conditions of this Agreement.

The terms and conditions of this Agreement may be updated or modified from time to time, and a condition of and in consideration of You being provided continued use of JNET, You must agree to the modified or updated terms and conditions. Failure to agree to any modified or updated terms and conditions will result in the termination of your access to JNET.

The content accessible through JNET derives from a variety of sources, each being a "data provider". You acknowledge that JNET is simply an identity service provider and a gateway to access content provided by JNET's data providers, and that JNET does not own, store, compile, develop, manage, or offer the content provided by JNET's data providers. You understand and agree that You are not being given a property or other right to JNET or to the content provided by JNET's data providers, and the Commonwealth of Pennsylvania may suspend, revoke, or terminate Your access to JNET for any reason. In addition, each data provider may suspend, revoke, or terminate Your access to its content for any reason.

This Agreement is in addition to any Federal, Commonwealth, or local laws and regulations, and any policies, directives and/or orders that effect or govern JNET or its data providers. If a conflict exists, the JNET Security Policy and the data provider policies shall control Your access to JNET and the data provider's content. You represent that You have been provided access to all JNET and data provider's policies, have read them and agree to comply with them. All JNET and data provider policies and procedure manuals are located at https://www.jnet.pa.gov/policies-manuals.

By accessing and using JNET you agree to:

1. Not to use any JNET resource or application or data provider content for unauthorized reasons such as personal or non-criminal justice or non-governmental purposes. Personal use is defined as querying or viewing JNET or data provider content that is not relevant to a criminal justice or official governmental purposes, including your own record(s) which is not authorized by JNET or its data providers.
2. Only release PennDOT photos to the press or the public when there is an active arrest warrant for a subject or a when a missing person report has been filed.
3. Immediately remove/recall released PennDOT photos from the newspaper, website, social media, etc. after a warrant has been cancelled or cleared or the missing person has been found.
4. Maintain the confidentiality of and safeguard all data provider content (whether in tangible or intangible form) in a manner consistent with JNETs and its data provider's policies and procedures.
5. Only disseminate data provider content within your own agency on a "Need to Know" or "Right to Know" basis for legitimate and official purposes consistent with this Agreement and JNET's and its

data provider's policies and procedures. Dissemination or disclosure of data provider content to the public or to unauthorized recipients is not permitted, unless otherwise specified by JNET or its data provider's policies.

6. Obtain authorization and complete all required training prior to accessing JNET applications.
7. Comply with JNET's and its data provider's policies, procedures, and standards.
8. Only use your own JNET username and password.
9. Obtain a JNET user id and password for each agency you work for.
10. Not to use an issued JNET user id and password from one agency while working at another agency.
11. Not to disclose your JNET user id and password to anyone.
12. Not to use or in any way enable anyone to use someone else's JNET username and password.
13. Immediately report unauthorized access or use of JNET or data provider content to the JNET Security Administrator.
14. Always supervise or secure your JNET session.
15. Use reputable anti-malware software.
16. Deploy an automatic screen lock with password/PIN for all devices accessing JNET independent of the JNET Username/Password.
17. Not use "rooted" or "jail broken" devices or systems where administrative privileges of the operating system have been altered.
18. Not to host internet access or create a hotspot on a device that is accessing JNET.
19. Not to access JNET via publicly accessible computers or kiosks at any time.
20. Obtain pre-authorization from your agency prior to using any personally owned devices (Phones, Laptops, Tablets and or PCs) to access JNET.
21. Not to use any personally owned devices (Phones, Laptops, Tablets, and or PCs) to access any JNET application that displays CLEAN, CJIS or PennDOT information, regardless of authorization status.
22. Not to transmit/disseminate Criminal Justice Information or Personal Identifiable Information (PII) (e.g., SSN's, DOB, SID, FBI#) via non-encrypted email (Gmail, Yahoo, Outlook.com, etc.) or via text messaging, even to authorized individuals.
23. Use known secure electronic communications when accessing JNET – no public Wi-Fi connections.
24. Notify your JNET Registrar of any name change, facility change, or job change.
25. Maintain documentation as required in the event of expungement orders (e.g., dissemination logs).
26. Report suspected misuse to the JNET Security Administrator.
27. Report any lost or stolen devices used to access JNET to your agency and the JNET Security Administrator.
28. Cooperate with misuse investigators from any entity with appropriate jurisdiction, including: your agency; any JNET data providers; JNET Office; Pennsylvania State Police, Pennsylvania Office of Attorney General; and/or Federal Bureau of Investigation.

Policy Violations:

In addition to the other rights of JNET and its data providers, which shall not be diminished by the following, your access to JNET or to data provider content may be suspended, revoked, or terminated immediately and without notice for:

- Violating any portion of this Agreement.
- Violating any of JNET's or its data provider's policies.

- Failing to cooperate with investigators during a misuse investigation.
- Using JNET access for unauthorized personal or Non-Criminal Justice or Non-Governmental Purposes

NOTE: *Policy violations may also result in criminal prosecution, and/or civil proceedings.*

No delay or failure on the part of the Commonwealth to exercise any right or power arising under this Agreement will act as a waiver of such right. If any of the provisions of this Agreement are held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, the validity, legality, and enforceability of the other provisions shall not be affected or impaired.

This Agreement supersedes all other agreements and understandings, both written and oral, between the parties with respect to the subject matter contained herein.

This Agreement shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. The courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Agreement and the resolution thereof. Any legal action relating to this Agreement must be brought in Dauphin County, Pennsylvania, and the parties agree that jurisdiction and venue in such courts is appropriate.

By electronically acknowledging this Agreement, the User certifies that the User has read, understands, and agrees to abide by the requirements of this Agreement. This electronic acknowledgement, including the date and time this agreement was acknowledged, is recorded at the JNET offices.