MEMORANDUM OF UNDERSTANDING

Traffic and Criminal Software (TraCS)

WITNESSETH

WHEREAS, The Panama City Police Department, hereafter referred to as PCPD, and the North Port Police Department, hereafter referred to as Contract Agency (CA), are both criminal justice agencies, formally recognized by the Federal Bureau of Investigation (FBI) and the Florida Department of Law Enforcement (FDLE), and;

WHEREAS, PCPD and the CA are headquartered within the boundaries of the State of Florida, and;

WHEREAS, both PCPD and the CA have entered in Criminal Justice User Agreements (UA) with FDLE and are required to abide by the current FBI Criminal Justice Information System (CJIS) Security Policy (CSP) for access to state and national Criminal Justice Information (CJI) as defined by the CSP, and;

WHEREAS, the FDLE CJIS Director functions as the CJIS Systems Officer (CSO) for the State of Florida, required by the CSP and UA to grant and authorize access to CJI within the State of Florida, and;

WHEREAS, PCPD presently has the benefit of contracting with TraCS Florida, a private vendor, operated and maintained by FSU, which provides access to TraCS, and;

WHEREAS, the CA wishes to utilize the PCPD FSU TraCS Systems for law enforcement purposes, and;

WHEREAS, PCPD is willing to share individual background screening information obtained from state and national fingerprint-based records checks with the CA, in a manner consistent with the requirements of the CSP;

NOW WHEREFORE, the parties agree as follows,

1. FSU will provide the PCPD with a current and complete list of all personnel who require unescorted physical or local access to CJI.

2. PCPD will ensure all personnel provided in Section 1, above, are appropriately screened and trained.

3. PCPD will fingerprint and submit the requisite identification information on personnel who require unescorted physical or local access to CJI prior to being granted access. PCPD will use its criminal justice ORI for submitting fingerprints required by the CSP and UA. PCPD will retain

the fingerprint-based records check, the signed security addendums, and the completed Security Awareness Level 4 certificates for said personnel.

4. PCPD will maintain a current and complete list of all personnel who have been authorized to access CJI. Individual information shall include name, date of birth, and if previously provided, Social Security Number or unique identification to accurately identify the individual.

5. PCPD shall provide to the CA the list of all personnel who are authorized access to CJI inside TraCS.

6. PCPD shall defer to the FDLE CSO regarding any issues with respect to CJI access eligibility as required by the CSP and UA.

7. When any change occurs to the list of authorized personnel, the PCPD shall provide to the CA the corrected or revised list of authorized personnel, and specifically identify any additions, deletions, or modifications to the list.

8. PCPD will notify the CA in the event that an individual, whether seeking or already authorized access to CJI, is denied such access by the FDLE CSO.

9. To properly assess any potentially disqualifying information as it becomes available, every year, PCPD shall perform a name-based check via the FCIC message switch, to include, but not limited to, hot files, and state/national criminal history record information searches, on all personnel authorized access to CJI in TraCS.

10. Upon notification/determination of any type of reported or observed criminal or other disqualifying activity by an individual authorized access to CJI in TraCS, the PCPD shall immediately notify the CA via formal correspondence of the individual's activity.

11. PCPD shall immediately notify the CA upon learning of the termination or suspension from employment of an individual authorized access to CJI in TraCS.

12. The CA shall be entitled to use, through agents and employees of the PCPD, the TraCS interface located at the PCPD for the purpose of gaining access to information Systems for law enforcement purposes.

13. The CA agrees to abide by all applicable local, state, and federal laws, rules and regulations, with regards to the use of any device accessing CJI and/or TraCS under the terms of this agreement.

14. The CA agrees to abide by all terms and conditions of the most recent UA executed into between FDLE and the CA.

15. The CA agrees that it shall make use of the TraCS access in compliance with the CSP.

16. If the CA intends to use mobile devices (as defined in the CSP), the CA agrees to have and operate a Mobile Device Management (MDM) solution as required by the CSP.

17. In compliance with the FDLE UA, the CA agrees to have a formal written policy restricting TraCS access to agency owned devices and forbidding access and use of TraCS on personally owned or public devices.

18. The CA grants PCPD permission to retain and host all records created inside TraCS by the CA in accordance with the CSP and FDLE UA.

19. The CA acknowledges that backups for all hosted records created inside TraCS by the CA are stored at the designated backup site of Clermont Police Department.

20. The CA grants PCPD and aforementioned personnel provided in section 1 permission to view and create records in FSU TraCS on behalf of the CA solely for the purposes of training or troubleshooting.

21. The CA agrees that neither PCPD nor the aforementioned personnel provided in section 1 are responsible for fulfilling public records requests on behalf of the CA. PCPD agrees to forward all public records requests it receives for records created and/or owned as described in section 19 by the CA to the CA.

22. The CA retains ownership of all records created inside TraCS by the CA and responses generated as a direct result of the CA, including user accounts, account access and audit logs, user activity, query history, and query responses, and agrees to fulfill any and all public records requests regarding those records.

23. PCPD agrees that the current Terminal Agency Coordinator (TAC) of the CA as recorded with FDLE and/or the current agency head within the CA shall be notified by PCPD of updates and information regarding personnel authorized to access CJI, including but not limited to when an individual is added or removed from the list of authorized users or when an individual on the list is arrested.

24. PCPD shall have formal written guidelines defining the processes associated with implementation of this Agreement.

25. PCPD will forward a copy of this Agreement of the FDLE CSO.

26. The term of this agreement shall commence on the date the Agreement is signed by both parties.

27. Either part may terminate this Agreement upon thirty (30) days written notice or immediately by PCPD without notice upon finding that the CA has violated terms of this Agreement, or immediately by the CA without notice upon finding that PCPD has violated the terms of this Agreement.

28. This agreement constitutes the entire agreement of the parties and may not be modified or amended without written agreement executed by both parties, and establishes procedures and policies that will guide all parties to comply and adhere to the CJIS Security Policy.

29. This Agreement supersedes all prior or contemporaneous negotiations, commitments, agreements (written or oral) and writings between PCPD and the CA with respect to the subject matter hereof. All such other negotiations, commitments, agreements and writings will have no further force or effect, and the parties to any such other negotiation; commitment, agreement or writing will have no further rights or obligations there under.

IN WITNESS HEREOF, the parties hereto have caused this Agreement to be executed by the proper officers and officials.

Panama City Police Department

Agency Name (PCPD)

Authorized Signatory (PCPD)

Scott Ervin #1999 Chief of Police

Printed Name / ID # Title

Witness (PCPD)

Printed Name / ID # Title

Agency Name (CA)

Authorized Signatory (CA)

Printed Name / ID # Title

Witness Signature (CA)

Printed Name / ID # Title

The current FBI CJIS CSP mandates all agencies connected to the FBI CJIS systems adhere to regulation set forth within the Security Policy. Included within the term "personnel" are all individuals who are utilized by criminal justice agencies to implement, deploy, and/or maintain the computers and/or networks of the criminal justice agency which are used to access FBI CJIS systems. These individuals include city/county IT personnel, and private vendors. The subject of non-criminal justice governmental personnel and private vendors is addressed in Sections 5.1.1.5(1) of the CJIS Security Policy, and the Security Addendum, which can be found in Appendix H.