THIRD-PARTY DATA SHARING AUTHORIZATION

This Third-Party Data Sharing Authorization (this "**Authorization**") is entered into as of **February 24, 2026**, between **the Hollywood Police Department, Florida** ("**Agency**") and Peregrine Technologies, Inc., a Delaware corporation with a mailing address at P.O. Box 7775 #69596, San Francisco, California 94120 ("**Peregrine**").

WHEREAS, Peregrine provides, among other products and services, a proprietary hosted real-time decision and operations management platform for use by public safety agencies (such as Agency) (the "**Peregrine Platform**");

WHEREAS, Agency is a Peregrine customer and user of the Peregrine Platform; and

WHEREAS, in accordance with the terms of this Authorization, Agency desires to share and receive certain law enforcement-related data ("**Law Enforcement Data**") via the Peregrine Platform with other Peregrine Public Law Enforcement customers within the following territories: **United States of America** (the "**Approved Law Enforcement Network**").

NOW, THEREFORE, in consideration of the mutual acknowledgements identified herein, Agency agrees as follows:

1. AUTHORIZED RELEASE OF LAW ENFORCEMENT DATA

A. Sharing of Law Enforcement Data:

Agency authorizes the sharing of Law Enforcement Data with Peregrine customers within the Approved Law Enforcement Network ("**Approved Agencies**") as permitted by applicable laws, rules, and regulations, and authorizes Peregrine to enable such sharing via the Peregrine Platform. Should Agency not want certain Law Enforcement Data to be made available to certain other Approved Agencies, Agency must identify the applicable Law Enforcement Data to Peregrine in writing and work together with Peregrine to restrict the sharing of that Law Enforcement Data with such Approved Agencies. The Peregrine Platform provides access controls that enable its customers (including Agency) to conceal any piece of Law Enforcement Data based on its record type (such as, but not limited to, Evidence, Person, or Vehicle), its record properties (such as, but not limited to, Case Number, Name, or Phone Number), and any combination thereof.

Agency shall work with Peregrine to articulate, in writing, the restrictions pertaining to the Approved Agencies allowed to access shared Law Enforcement Data and the data types not to be shared with other Approved Agencies (the "**Sharing Framework**"). The Sharing Framework is a precondition to enabling and implementing data sharing in the Peregrine Platform and must be finalized prior to the activation of the data sharing feature. Agency shall obtain any third-party consents or approvals necessary to enable the sharing of such Law Enforcement Data in accordance with this Authorization and the Sharing Framework.

For purposes of clarity, this Authorization does not require Agency to share Law Enforcement Data with any other Peregrine customer.

B. Limitation on Law Enforcement Data Sharing:

Agency shall only share or release Law Enforcement Data to authorized representatives of Approved Agencies who have an approved login and password to the Peregrine Platform ("**Authorized Users**") and who have a need and/or right to

DRAFT

know information contained within the Law Enforcement Data under the Sharing Framework.

Agency retains the right to withhold any specific record or any category of records from being shared for any reason and at any time, either by independently restricting records or by requesting Peregrine to do so. Any disputes or requests to share withheld records shall be resolved between the appropriate authorized personnel of Agency and each Approved Agency under any applicable laws, rules, regulations, policies and standards.

C. **Compliance with Laws:**

Agency acknowledges that Peregrine's customers are generally subject to laws, rules, regulations, policies, and standards requiring public disclosure of certain government materials, meetings, and records ("**Sunshine Laws**"). While Law Enforcement Data shared via the Peregrine Platform via this Authorization will be subject to such Sunshine Laws to the extent applicable, Agency agrees to use reasonable efforts to ensure any Law Enforcement Data received from another Approved Agency is maintained as confidential and only Authorized Users shall be permitted to obtain the applicable Law Enforcement Data. Any Law Enforcement Data obtained by Agency shall only be used for purposes that are consistent with existing law. Agency does not waive any exemption under any Sunshine Laws or any other laws, rules, regulations, policies, or standards that may apply to the Law Enforcement Data.

Further, Agency acknowledges that sharing Law Enforcement Data via the Peregrine Platform in accordance with this Authorization is subject to the applicable laws, rules, regulations, policies, and standards of the jurisdiction in which Agency is based controlling the release of information, access control, retention of records and reporting duties. Agency acknowledges that it is Agency's and each other Approved Agency's obligation to comply with the foregoing connection with the sharing of Law Enforcement Data with each other over the Peregrine Platform.

2. LAW ENFORCEMENT DATA OWNERSHIP

A. **Ownership:**

Agency retains ownership of all of its respective Law Enforcement Data. Agency and each other Approved Agency is responsible for creating, updating, and deleting data (including Law Enforcement Data) in its own systems of record according to its own retention policies. Agency shall make reasonable efforts to ensure the completeness and accuracy of its Law Enforcement Data.

B. **Release of Information:**

Agency shall authorize the release of Law Enforcement Data only to Approved Agencies authorized under the Sharing Framework to receive such Law Enforcement Data. Agency represents and warrants that it will not release or otherwise share Law Enforcement Data with any third party except as expressly authorized by the Approved Agency that owns, created, or originated the requested Law Enforcement Data ("**Source Agency**")..

C. **Unauthorized Requests:**

If Agency receives a request for Law Enforcement Data stored on the Peregrine Platform by anyone who is not authorized to receive such Law Enforcement Data

DRAFT

under the Sharing Framework, Agency shall refer the request to the Source Agency.

D. **Public Record Requests, Subpoenas and Court Orders:**

If Agency receives a public records request, subpoena, or court order ("**Legal Request**") for Law Enforcement Data that was not owned, created, or originated by it, Agency shall refer the requestor to the appropriate Source Agency.

3. USER ACCESS

A. **Login Application Process:**

Agency shall designate an Authorized User with administrative privileges to govern its Law Enforcement Data-sharing policy (the "**Manager**"). The Manager is responsible for managing permissions and access regarding Law Enforcement Data sharing for each Authorized User. Agency agrees that Authorized Users shall be limited to current authorized representatives who are legally authorized to review criminal history data for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Manager or their designee. The Manager shall have the sole discretion to deny or revoke individual access for Agency's Authorized Users.

B. **Login Assignment:**

Each Authorized User will be issued a user login and a password by the Manager. Authorized Users may be assigned to groups that have varying levels of access rights based on their roles and functions within Agency's organization, as well as the level of sensitivity or restriction applicable to different pieces of data or information.

C. **Termination of Logins:**

Manager is responsible for the timely removal of any login accounts associated with Authorized Users who leave Agency, no longer qualify for access to the Peregrine Platform, or are denied access by the Manager for any other reason.

D. **Intended Use:**

Agency shall ensure that each Authorized User utilizes Law Enforcement Data received from other Approved Agencies solely for law enforcement purposes and in accordance with applicable laws, rules, regulations, policies, and standards and any authorized purpose.

E. **Limitations on Use of Logins:**

Agency shall ensure that each Authorized User shall not access Law Enforcement Data by using a name or password that was assigned to another Authorized User. Agency will ensure that each Authorized User does not give his or her password to any other person, including another Authorized User, to access the Peregrine Platform.

F. **Audit Trail:**

Each action taken by an Authorized User (such as, but not limited to Searches, Downloads, Shares, and Views) will be logged in the Peregrine Platform and will include a Case Number where applicable in an audit trail of Authorized User actions. Any requests for the audit logs of transactions taken in the Peregrine Platform made by Authorized Users, representatives internal to Agency (such as, but not limited to

DRAFT

Internal Affairs personnel, supervisory personnel, or Records staff), or elected bodies overseeing Agency (such as, but not limited to a County Board of Supervisors or City Council) shall be made in writing to the Manager, who shall provide the logs to the requestor within a reasonable amount of time and in accordance with applicable laws. Manager (or their designees) will conduct routine reviews of all audit information to confirm that the Law Enforcement Data conducted hereunder sharing maintains compliance with applicable Agency policies. The frequency and content of these reviews will be determined by each Manager, based on relevant applicable state law.

G. **CJIS Compliance:**

Agency and all Authorized Users shall comply with the U.S. Department of Justice Criminal Justice Information Services Security Policy ("**CJIS Policy**"), including any revisions to the CJIS Policy that may be implemented after the Effective Date of this Authorization.

4. CONFIDENTIALITY OF INFORMATION

A. **Law Enforcement Data Confidentiality:**

Information in a Peregrine Platform account is confidential and is not subject to public disclosure, except as required by applicable law. Only Authorized Users are allowed to view and use the information in a Peregrine Platform account. Otherwise, the Law Enforcement Data shall be kept confidential for purposes of not compromising active investigations or undercover operations, or otherwise jeopardizing officer or public safety, or Agency's ability to perform its duties.

B. **Internal Requests for Law Enforcement Data:**

An Authorized User who receives a request from a non-authorized requestor for information in a Peregrine Platform account shall not release that information but may instead refer the requestor to the Source Agency.

C. **Removal or Editing of Records:**

Agency and each Approved Agency shall determine their own schedule for record deletion and other edits to their own data in their systems of record. This will be determined by the Agencies' policies and/or applicable legal requirements.

5. RELATIONSHIP TO CUSTOMER AGREEMENT

A. For clarity, the terms of this Authorization do not modify or otherwise affect the terms of any subscription agreement or other agreement in place between Agency and Peregrine (the "**Peregrine Agreement**") except that Agency agrees that, notwithstanding any term of any Peregrine Agreement, Peregrine's enablement of and activities with respect to the activities described in this Authorization shall not be considered a breach of the Peregrine Agreement. This Authorization will otherwise be subject to, and is governed by, the terms and conditions of the Peregrine Agreement (as modified by this Authorization).

B. Agency acknowledges that Peregrine has indicated that it will implement this Authorization once signed and will use reasonable efforts to implement any modifications or requests from Agency and other Approved Agencies with regard to the Sharing Framework for the duration of this Authorization.

6. EFFECTIVENESS OF AUTHORIZATION

DRAFT

This Authorization will commence upon its execution by Agency. It may be terminated at any time, with or without notice, by Agency or Peregrine revoking Law Enforcement Data sharing access from Agency and/or all other Approved Agencies (as applicable).

7. COUNTERPARTS

This Agreement may be signed in counterparts, each of which shall be deemed to be an original. The Parties agree that the digital signatures of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as manual signatures. Any digital signature shall have the same legal validity and enforceability as a manually executed signature or use of a paper-based record keeping system to the fullest extent permitted by applicable law.

8. SIGNATURES.

The individual executing this Authorization represent and warrant that they have the right, power, legal capacity, and authority to enter into and to execute this Authorization on behalf of Agency and Peregrine, respectively.

Authorized by:

_____ Date: _____

[TITLE]

[AGENCY NAME]

Authorized by:

_____ Date: _____

Peregrine Technologies, Inc.

DRAFT