RATIFICATION OF PEREGRINE SOFTWARE AGREEMENT

Peregrine is a new software system purchased through our affiliation with PRIME (Pinellas Regional Information Management Enterprise). PRIME is a county organization we are a member of and is the entity driving our new countywide CAD and reporting system. Our membership is paid through our annual agreement with the Sheriff's Office.

FDLE requires an agency to be the LEAD when multiple agencies share reporting and sometimes confidential information between agencies. In this case, Largo took the lead for the Peregrine software system and all the other agencies are users.

I am asking the commission to ratify our participation and use of the system to satisfy our FDLE requirements. Peregrine allows our agency to access other Pinellas County law enforcement agencies reports in real time, enhancing our investigative process across jurisdictions.

Memorandum of Understanding

Pinellas County Shared System "Peregrine" Lead Agency/Solution Agreement

WHEREAS, The Largo Police Department hereafter referred to as Lead Contract Agency (LCA), and the following Criminal Justice Agencies: Pinellas County Sheriff's Office, Clearwater Police Department, St. Petersburg Police Department, Pinellas Park Police Department, Treasure Island Police Department, Indian Shores Police Department, Pinellas County School Board Police Department, Gulfport Police Department, Tarpon Springs Police Department, Belleair Police Department, and Kenneth City Police Department, hereafter referred to as Contract Agencies (CA), are all criminal justice agencies, formally recognized by the Federal Bureau of Investigation (FBI) and the Florida Department of Law Enforcement (FDLE); and

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

WHEREAS, both the LCA and CA have entered into Criminal Justice User Agreements (UA) with FDLE and are required to abide by the FBI CJIS [Criminal Justice Information Systems] Security Policy (CJISSECPOL) for access to state and national Criminal Justice Information (CJI) as defined by the CJISSECPOL; and

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

WHEREAS, both the LCA and CA are currently contracting with and have a contract for services with *Peregrine,* a private company, for services supporting the administration of criminal justice and systems containing CJI; and

WHEREAS, the CJISSECPOL requires criminal justice agencies to execute a Vendor Contract with non-governmental entities who are contracted to provide services with access to criminal history record information in support of the administration of criminal justice; and

WHEREAS, Peregrine is required to adhere to the FBI CJIS Security Policy Security Addendum Process,

WHERAS, the LCA is willing to share Peregrine employee background screening information obtained from state and national fingerprint -based records checks with the CA, in a manner consistent with the requirements of the CJISSECPOL;

NOW THEREFORE, the parties agree as follows,

1. The LCA will fingerprint, submit, and retain the requisite identification information on Peregrine employees who require unescorted physical or logical access to CJI and/or CJI Systems and Networks. The LCA will use its criminal justice ORI for submitting fingerprints required by the CJISSECPOL and UA.
2. The LCA will maintain a current and complete list of all Peregrine employees who have been authorized access to CJI. Employee information shall include name, date of birth, social security number, date fingerprinted, as well as the date initially trained, tested, certified, or recertified.
3. The LCA shall provide to the CA the list of all Peregrine employees who are authorized access to CJI.
4. When any change occurs to the list of authorized Peregrine employees, the LCA shall provide to the CA the corrected or revised list of authorized Peregrine employees, and specifically identify any additions, deletions, or modifications to the list.
5. The LCA will notify the CA if an employee of Peregrine, whether seeking or already authorized access to CJI, is denied such access by the FDLE CSO.
6. Upon notification/determination of any type of reported or observed criminal or other disqualifying activity by ana Peregrine employee authorized access to CJI, the LCA shall immediately notify the CA via formal correspondence of the employee activity.
7. The LCA shall immediately notify the CA upon learning of the termination or suspension from employment of a Peregrine employee authorized access to CJI.
8. The LCA shall ensure Peregrine employees complete appropriate security awareness training as identified in the CJISSECPOL.
9. The LCA shall ensure Peregrine employees sign the CJIS Security Addendum Certification Page and shall retain those copies as required by the FBI CJIS Security Policy and the FDLE User Agreement.
10. In the event that Peregrine outsources any work to a third-party vendor or contractor, the LCA will be responsible to ensure that all vendor employees are fingerprinted under the LCA's ORI, take and maintain appropriate level of Security Awareness Training, maintain a signed security addendum certification page of all vendor personnel, maintain the required vendor personnel personal information (as outlined under 2) and provide all the information to the CA as it pertains to their systems or equipment.
11. The CA shall designate a primary and secondary point of contact within its agency to receive information and updates regarding Peregrine and any third-party vendors/contractors of the Peregrine employees authorized to access CJI.
12. The LCA shall defer to the FDLE CSO regarding any issues with respect to CJI access eligibility as required by the CJISSECPOL and the U/A.

13. The LCA shall have formal written guidelines defining the processes associated with implementation of this Agreement.
14. The LCA will forward a copy of this agreement to the FDLE CSO.
15. Either party may terminate this agreement upon thirty (30) days written notice to the other.
16. This Agreement constitutes the entire agreement of the parties and may not be modified or amended except by written amendment signed by authorized representatives of both parties.
17. Both parties acknowledge that the CJI authorized to be shared by this Agreement is subject to restrictions on access and dissemination under federal and state law, and that failure to abide by those restrictions can result in loss of access to CJI.

Cloud Implementation and Solution Review

1. As the LCA, Largo Police Department submitted a cloud implementation plan and completed vendor questionnaire for the Peregrine system, housed within the AWS Government Cloud.
2. The LCA is responsible for ensuring the overall compliance with the system as it relates to the control families outlined within the CJIS Security Policy.
3. Prior to implementation, the system was reviewed with the requirements of version 5.9.5 of the CJIS Security Policy.
4. Updates and changes to the system because of changes made to the CJIS Security Policy will be the responsibility of the LCA to ensure the vendor updates the system to new requirements.

Audit Logs, Multi-Factor Authentication, and Mobile Devices

1. Each member of the CA is responsible to ensure they have a Peregrine administrator who is responsible for account management and audit log review.
2. Each member of the CA is responsible to have access to and review audit logs within the Peregrine system for their agency users.
3. Each member of the CA is responsible to ensure compliant multi-factor authentication is in place and enforced prior to access to CJI, including the Peregrine system.
4. If a member of the CA intends to use limited featured operating system devices for access to the Peregrine system, the CA member is responsible for ensuring all requirements of the mobile device section is meet as outlined within the CJIS Security Policy.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their authorized representatives, effective on the date last signed.

Belleair Police Department (CA Member Agency)

Richard "Rick" J. Doyle, Chief of Police — Date 4/23/25

Witness — Date 4/23/2025