

**PALM BEACH COUNTY
BOARD OF COUNTY COMMISSIONERS
AGENDA ITEM SUMMARY**

Meeting Date: July 10, 2018

[X] Consent
[] Ordinance

☐ Regular
☐ Public Hearing

Department: Department of Public Safety
Submitted By: Department of Public Safety
Submitted For: Division of Consumer Affairs

I. EXECUTIVE BRIEF

Motion and Title: **Staff recommends motion to receive and file:** Volunteer & Employee Criminal History System (VECHS) User Agreement with the Florida Department of Law Enforcement (FDLE), which authorized the Department of Public Safety Division of Consumer Affairs (DCA) to process “level 2” criminal history background checks on home caregiver applicants.

Summary: The DCA received a request from the FDLE to sign a new VECHS User Agreement to enable DCA to process “level 2” criminal history background checks on home caregiver applicants using live scan technology to submit fingerprints to the FDLE and Federal Bureau of Investigation (FBI) databases. The new agreement includes non-substantive changes compared to the agreement currently in place, which was approved by the Board of County Commissioners on March 1, 2016, (R2016-0299). The agreement outlines the responsibilities of both parties to include retention of applicant fingerprints, notification program, privacy, and security. R2018-0582 authorized the County Administrator or designee to sign future VECHS applications, user agreements, amendments and/or renewals for criminal history background checks on home caregivers with FDLE. Countywide (LDC)

Background and Justification: On October 20, 2015, the Board of County Commissioners approved the Home Caregiver Ordinance requiring licensure of Home Caregivers. The ordinance authorized DCA to run “Level 2” fingerprint based national history criminal background checks through the FDLE and FBI databases on applicants. The agreement currently in place was approved by the Board of County Commissioners on March 1, 2016, (R2016-0299). DCA received a request from the FDLE to sign a new VECHS application following the review of and approval of an updated VECHS application. Approximately 1,300 fingerprints were submitted to the FDLE and FBI under the Home Caregiver program. Home Caregiver applicants pay the costs associated with the fingerprint based criminal history check as outlined in the fee resolution.

Attachment:

- ## 1) VECHS User Agreement

Recommended by: *[Signature]* 6/13/18
Department Director Date

Approved By:  4/25/18
Assistant County Administrator Date

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact

Fiscal Years	<u>2018</u>	<u>2019</u>	<u>2020</u>	<u>2021</u>	<u>2022</u>
Capital Expenditures	_____	_____	_____	_____	_____
Operating Costs	_____	_____	_____	_____	_____
External Revenues	_____	_____	_____	_____	_____
Program Income (County)	_____	_____	_____	_____	_____
In-Kind Match (County)	_____	_____	_____	_____	_____
Net Fiscal Impact	_____*	_____	_____	_____	_____

ADDITIONAL FTE

POSITIONS (Cumulative) _____

Is Item Included In Current Budget? Yes _____ No _____

Does this item include the use of federal funds? Yes _____ No X

Budget Account Exp No: Fund _____ Department _____ Unit _____ Object _____

Rev No: Fund _____ Department _____ Unit _____ Rev Source _____

B. Recommended Sources of Funds/Summary of Fiscal Impact:

Grant:

Fund:

Unit:

*Revenue is derived from payments made by home caregiver applicants as outlined in the fee resolution which offsets the cost for the criminal history record checks and fingerprint retention fees paid to FDLE.

Departmental Fiscal Review: _____

III. REVIEW COMMENTS

A. OFMB Fiscal and/or Contract Dev. and Control Comments:

Robert P. P. 6/15/18
9/10
4/14 OFMB 7/6/14

Don J. Jacobs 6/20/18
Contract Administration

B. Legal Sufficiency:

7/10/18 6/20/18
Assistant County Attorney

C. Other Department Review:

Department Director

This summary is not to be used as a basis for payment.



Criminal Justice Information Services
User Services Bureau

VECHS USER AGREEMENT

Volunteer & Employee Criminal History System (VECHS) for
Criminal History Record Checks by a Qualified Entity under the
National Child Protection Act of 1993, as amended, and
Section 943.0542, Florida Statutes

I. Parties to Agreement

This Agreement, entered into by the Florida Department of Law Enforcement (hereinafter referred to as FDLE), an agency of the state of Florida, with headquarters in Tallahassee, Florida, and PALM BEACH COUNTY BOARD OF COUNTY COMMISSIONERS - DIVISION OF CONSUMER AFFAIRS with entity number: E/V 50010002 (hereinafter referred to as User), located at 50 SOUTH MILITARY TRAIL, SUITE 201, WEST PALM BEACH, FL 33415 is intended to set forth the terms and conditions under which criminal history record checks authorized by the National Child Protection Act of 1993, as amended, (hereafter referred to as the NCPA), and as implemented by Section 943.0542, Florida Statutes (F.S.), shall be conducted.

- A. FDLE has established and maintains intrastate systems for the collection, compilation, and dissemination of state criminal history records and information in accordance with Subsection 943.05(2), F.S., and, additionally, is authorized and does participate in similar multi-state and federal criminal history records systems pursuant to Subsection 943.05(2), F.S.
- B. FDLE and its user agencies are subject to and must comply with pertinent state and federal laws relating to the receipt, use, and dissemination of records and record information derived from the systems of FDLE and the U.S. Department of Justice (DOJ) (Chapter 943, F.S., Chapter 11C-6, F.A.C., 28 C.F.R. Part 20).
- C. User is a business or organization, whether public, private, operated for profit, operated for not for profit, or voluntary entity operating within the state of Florida, which provides care or care placement services, or licenses or certifies others to provide care or care placement services. As such, the User is authorized to submit fingerprints and review resultant criminal history records as part of the screening process for its current and/or prospective employees and volunteers (which classes of persons shall be understood for purposes of this Agreement to include contractors and vendors who have or may have unsupervised access to the children, disabled, or elderly persons for whom User provides care), pursuant to Section 943.0542, F.S., and the NCPA, and forms the legal basis for User's access to criminal history record information derived from the systems of the DOJ.

Revised 3/14/2018

Attachment # 1

Page 1 of 11

- D. If the User is a governmental entity (e.g., city or county) with more than one functional unit (e.g., department, division, bureau, or office), the User will not be treated as a single qualified entity for purposes of participation in the VECHS program. Rather, each functional unit will be assigned its own account and corresponding Originating Agency Identifier (ORI) and will be treated as a separate and distinct qualified entity. Accordingly, fingerprints submitted on current or prospective employees and volunteers must be identified as coming from the functional unit with which the employee or volunteer is or will be associated (e.g., Parks and Recreation). The VECHS account assigned to one functional unit within the governmental entity cannot be used to submit fingerprints for other functional units within the same governmental entity.
- E. The National Crime Prevention and Privacy Compact (Compact) Act of 1998 established an infrastructure by which states can exchange criminal records for non-criminal justice purposes according to laws of the requesting state and provide reciprocity among the states to share records without charging each other for the information. The Compact also established a Council to monitor the effective use of the Interstate Identification Index (III) system for Federal-State exchange to ensure rules and procedures for effective and proper operations for Non-Criminal Justices purposes. The Council requires each state to adhere to national standards concerning record dissemination, use, system security, and other duly established standards, including those that enhance the accuracy and privacy of such records. The Federal Bureau of Investigation (FBI) shall conduct a triennial audit of each state to ensure compliance with Compact policies. Failure to remain compliant with Compact policies by each state could result in sanctions levied by the Council or ultimately loss of access to criminal history information contributed by other states through the III.
- F. User is desirous of obtaining and FDLE is required and willing to provide such services so long as proper reimbursement is made and all applicable federal and state laws, rules, and regulations are strictly complied with.
- II. Now, therefore, in light of the foregoing representations and the promises, conditions, and terms, more fully set forth hereinafter or incorporated by reference and made a part hereof, FDLE and User agree as follows:
- A. FDLE agrees to:
1. Assist User concerning the privacy and security requirements imposed by state and federal laws; provide User with copies of all relevant laws, rules, and/or regulations as well as updates as they occur; offer periodic training for User's personnel.
 2. Provide User with such state criminal history records and information as reported to, processed, and contained in its systems and legally available to the User.
 3. Act as an intermediary between User and the DOJ, securing for the use and benefit of User such federal and multi-state criminal history records or information as may be available to User under federal laws and regulations.

Revised 3/14/2018

Attachment # 1
Page 2 of 11

B. User agrees to:

1. Provide FDLE with properly executed applicant fingerprint submissions.
2. Submit requests to FDLE for criminal history record checks pursuant to this agreement only for User's current and prospective Florida employees and volunteers, for whom User is not already required to obtain state and national (Level 2) criminal history record checks under any other state or federal statutory provision. User shall continue to comply with all other such statutory provisions for all applicable persons.
3. Determine whether the current or prospective employee or volunteer has been convicted of, or is under pending indictment for, a crime that bears upon his or her fitness to have access to or contact with children, the elderly, or individuals with disabilities or to have to have responsibility for their safety and well-being.
4. Obtain a completed and signed Waiver Agreement and Statement form from every current or prospective employee and volunteer, for whom User submits a request for a criminal history record check to FDLE. FDLE will provide the Waiver Agreement and Statement form to the User for dissemination. (The signed Waiver Agreement and Statement allows the release of state and national criminal history record information to the qualified entity.) The Waiver Agreement and Statement must include the following: (a) the person's name, address, and date of birth that appear on a valid identification document (as defined at 18 U.S.C. § 1028); (b) an indication of whether the person has or has not been convicted of a crime, and, if convicted, a description of the crime and the particulars of the conviction; (c) a notification to the person that User may request a criminal history record check on the person as authorized by Section 943.0542, F.S., and the NCPA; (d) a notification to the person of his or her rights as explained in paragraphs 12-16 below; and (e) a notification to the person that, prior to the completion of the criminal history record check, User may choose to deny him or her unsupervised access to a person to whom User provides care. User shall retain the original of every Waiver Agreement and Statement form and make available to FDLE upon request.
5. ****IF USER IS PRIVATE, FOR PROFIT OR NOT FOR PROFIT**** – Pay for services provided by FDLE and the FBI in accordance with Rule 11C-6.004, F.A.C., with the submission of fingerprints.
6. ****IF USER IS A GOVERNMENTAL AGENCY**** – If User has set up a billing account with FDLE for services requested pursuant to this agreement, User will reimburse FDLE, in a timely fashion, in accordance with Rule 11C-6.004(3), F.A.C., upon proper presentation of billing for state services rendered and reimburse the FBI, in a timely fashion via FDLE, upon proper presentation of billing for federal services rendered. If User is not on a billing account, User shall pay for services provided by FDLE and the FBI in accordance with Rule 11C-6.004, F.A.C., with the submission of requests for criminal history record checks.

Revised 3/14/2018

Attachment # 1
Page 3 of 11

7. ****IF USER IS A GOVERNMENTAL AGENCY**** – Maintain adequate records, and monitor and allocate funds for payment of services under this agreement.
8. Ensure that User personnel authorized to receive and handle criminal history information are made aware of the requirements outlined in this agreement.
9. Promptly advise FDLE of any violations of this agreement.
10. Maintain an updated Agency Contact Form with FDLE and provide upon request.
11. Share criminal history information with other qualified entities only after confirming with FDLE that the requesting entity has been designated a qualified entity and has signed a user agreement, and only after verifying that the current prospective employee or volunteer has authorized the release of his or her criminal history records, if any, to other qualified entities by a statement on his or her signed waiver. User will respond that it is unable to provide any information to the requesting entity if the current or prospective employee or volunteer has requested that his or her criminal history record (s) not be released to any other qualified entity.
12. Provide to the applicant written notice that his/her fingerprints will be used to check the criminal history records of FDLE and the FBI.
13. When a determination of the applicant's suitability for the job, license, or other benefit is based solely on the FDLE or FBI criminal history, provide the applicant the opportunity to complete or challenge the accuracy of the information in the record.
14. Advise the applicant that procedures for obtaining a change, correction, or updating of an FDLE or FBI criminal history are set forth in F.S. 943.056 and Title 28, Code of Federal Regulations (CFR), § 16.34. The User may provide a copy of the applicant's criminal history to the applicant for their review and possible challenge.
15. Afford the applicant a reasonable time to correct or complete the record, unless the applicant has declined to do so, before denying a job, license, or other benefit based on information in the FDLE or FBI criminal history.
16. Establish and document the process/procedure it utilizes for how/when it gives the applicant notice, what constitutes "a reasonable time" for the applicant to correct the record, and any applicant appeal process that is afforded the applicant.

III. Retention of Applicant Fingerprints For Applicant Fingerprint Retention and Notification Program (AFRNP) Participating Users

- A. User officially requests, and FDLE agrees, to enter and retain in the Biometric Identification System (BIS) the applicant fingerprints submitted for state and national criminal history record checks, by Users having specific statutory authorization, to participate in the AFRNP

Revised 3/14/2018

Attachment # 1
Page 4 of 11

for current and prospective employees, contractors, volunteers, and persons seeking to be licensed or certified.

- B. User acknowledges that, pursuant to Section 943.05(3), F.S., retained fingerprints will be available for all purposes and uses authorized for arrest fingerprint submissions entered into BIS pursuant to Section 943.051, F.S.
- C. Upon User's submission of such applicant fingerprints in a digitized format acceptable to FDLE for entry into BIS, FDLE agrees that the fingerprints will be retained.
- D. Users submitting applicant fingerprints in accordance with Sections 943.05(g)-(h) and 943.0542, F.S., shall notify each person fingerprinted that his or her fingerprints will be retained for participation in the AFRNP and that the applicant's fingerprints will be retained by FDLE.
- E. FDLE agrees to search all arrest fingerprint submissions received under Section 943.051, F.S., against the fingerprints retained in BIS. When the subject of fingerprints submitted for retention under this program is identified with fingerprints from an incoming Florida arrest, as confirmed by fingerprint comparison, FDLE shall advise the User which submitted the applicant fingerprints of the arrest in writing (or other manner prescribed by FDLE). User acknowledges that arrests made in other states or by the federal government will not result in notification by FDLE, as User's access to these arrests is restricted by federal law. The information on arrests for these applicants in other states and by the federal government is available only upon a fingerprint submission to FDLE which will be forwarded to the FBI. User further acknowledges that, while it is not expected to be a frequent occurrence, if the submitted fingerprints for an applicant are of sub-standard quality or if the fingerprints submitted on an arrested individual were of sub-standard quality, the identification of these persons as the same may not occur and an arrest notification may not be made. User agrees that, until the arrest fingerprint submission is received by FDLE, FDLE will not identify the arrested person as the same individual retained in AFRNP.
- F. User agrees to remit an annual fee for participation in the AFRNP of \$6 per individual record retained. The initial entry of an applicant's fingerprints into the AFRNP database must be accompanied by a state and national criminal history record check. There is no additional fee for the first year of participation in the program. For each succeeding year, the \$6 per record annual fee will be charged. Users will be billed for this fee annually in advance on the anniversary month of the fingerprint record retention.
- G. The User acknowledges that its failure to pay the amount due on a timely basis or as invoiced by FDLE may result in the refusal by FDLE to permit the User to continue to participate in the fingerprint retention and search process until all fees due and owing are paid.
- H. Managing applicant fingerprints and billing:

The User agrees to inform FDLE in writing or electronically, and receive written confirmation from the FDLE, of all persons previously submitted by the User with retained fingerprints who

Revised 3/14/2018

Attachment # 1
Page 5 of 11

are no longer employed, licensed, certified, or otherwise associated with the User in order that such persons may be removed from the AFRNP.

There are two types of Users that manage retained fingerprints. Currently, some Users have direct access to manage fingerprints within the AFRNP database. Other Users do not have direct access to the system and communicate requests manually to FDLE through the Supplemental Authorization Form for Retained Applicant Deletions.

1. For Users with direct access: Prior to the payment of any individual retention fee, the User may inform FDLE in writing (or other manner prescribed by FDLE) of any person with retained fingerprints who is no longer employed, licensed, certified, or otherwise associated with the User in order that such person may be removed from the AFRNP database. With respect to any person previously entered in the database for which FDLE does not receive notification of removal within a minimum of ten days prior to the anniversary date of the entry the annual fee must be paid.
2. For Users without direct access: Prior to the payment of any individual retention fee, the User may inform FDLE in writing (or other manner prescribed by FDLE) of any person with retained fingerprints who is no longer employed, licensed, certified, or otherwise associated with the User in order that such person may be removed from the AFRNP database. With respect to any person previously entered in the database for which FDLE does not receive payment or notification of removal by the date specified on the invoice, the applicant fingerprints may be deleted.

IV. Privacy and Security

- A. User shall use criminal history record information acquired hereunder only to screen User's Florida current and/or prospective employees and/or volunteers, and only for purpose(s) of employment and/or determination of suitability for access to children, elderly, or disabled persons, pursuant to the terms of the NCPA of 1993, as amended, and Section 943.0542, F.S. If User is a governmental agency, such records may additionally be used in administrative hearings associated with one of the enumerated purposes.
- B. User shall not duplicate and/or disseminate criminal history records acquired hereunder for use outside of User entity except as authorized by state and federal law. Sharing of criminal history records with other qualified entities is permitted by the FBI provided that:
 1. Such other entity is authorized to receive criminal history record information derived from the systems of the DOJ in the manner specified herein and User has verified the other entity's qualifying status as required herein.
 2. User has been approved to receive criminal history record information pursuant to specific statutory authority and shall not use criminal history record information acquired pursuant to such approval for any other purpose, pursuant to 28 CFR 50.12.
- C. Criminal history record information received based on a fingerprint based criminal history record should be considered current only at the time at which it was received.

Revised 3/14/2018

Attachment # 1
Page 6 of 11

- D. Original Waiver Agreement and Statement form must be retained by User for as long as the employee or volunteer is working for User, or for five years, whichever is longer.
- E. User shall keep criminal history records acquired hereunder in a secure file, safe, or other security device, such as locked file cabinet in an access-controlled area, and shall take such further steps as are necessary to ensure that the records are accessible only to those of authorized employees who have been trained in their proper use and handling and have a need to examine such records.
- F. ****IF USER IS SUBJECT TO THE PUBLIC RECORDS ACT**** – A Florida criminal history record that is accessed by a state or local agency or qualified entity, under a regulatory statute approved by the FBI under P.L. 92-544 or under the NCPA/VCA as implemented in Florida by Section 943.0542, F.S., is not divisible into a state component that would be a public record under Section 943.053(3), F.S., and a national component that would be restricted under 28 C.F.R. s. 20.33. If a public record request is received by the accessing agency or qualified entity for such a record or records, FDLE will assist and work directly with the agency or qualified entity in responding to the request, and to any claim, demand, or suit, formal or informal, challenging that response, including any appeals. User shall not release any criminal history information that is made confidential or exempt from public records disclosure by law. In particular, record information derived from the DOJ shall not be disseminated to a non-qualified entity or used for a purpose other than that specified in the statute authorizing the request, Section 943.0542, F.S.
- G. When FDLE is auditing non-criminal justice agencies, the entirety of the FBI CJIS Security Policy (CSP) will be used to establish compliance. Appendix J of the CSP is a guideline which identifies specific areas of compliance for non-criminal justice agencies. This policy can be found at the FDLE website www.FDLE.state.fl.us. Significant areas are listed below:
1. Local Agency Security Officer (LASO) – User shall appoint a LASO to function as the point of contact in regard to security and audit related issues. The LASO shall coordinate CSP compliance for the User. (CSP section 3.2.9)
 2. Agency User Agreements – CSP requires that FDLE have an agreement with the User that ensures compliance with the CSP (CSP section 5.1.1.6). Acceptance of this Agreement signifies the VECHS User's agreement to comply with the CSP.
 3. Security and Management Control Outsourcing Standard – Outsourcing which would allow an external entity to access criminal history information obtained and/or maintained by User is not allowed. User shall contact FDLE to obtain approval prior to entering into a contract or granting limited criminal history information access to another entity for purposes of creating or maintaining the computer system(s) needed to accept or house criminal history information. (CSP section 5.1.1.7)
 4. User agrees not to store criminal justice information obtained through the VECHS program outside the state of Florida.

Revised 3/14/2018

Attachment # 1

Page 7 of 11

5. Secondary Dissemination – User agrees to only release/allow access to authorized User personnel or other qualified VECHS entities confirmed through FDLE, pursuant to 28 CFR 50.12. Each dissemination of criminal history information outside the authorized VECHS entity shall be documented in a dissemination log. (CSP section 5.1.3) This log shall include at a minimum:
 - a. Date of Dissemination
 - b. Applicant's Name
 - c. Provider's Name (Released By)
 - d. Requestor's Name & Agency (Released To)
 - e. SID/FBI Numbers
 - f. Reason for Dissemination (Why was this information requested? For what purpose?)
 - g. How the information was disseminated (e.g. encrypted email, fax, certified mail, etc.)
6. Security Awareness Training – User shall ensure that all persons who access/process/read, or maintain criminal history information or the systems used to process/store criminal history information, complete, within six months of initial assignment, and biennially thereafter, the appropriate FDLE CJIS Online security awareness training. This security awareness training can be accessed through the FDLE website at www.FDLE.state.fl.us. (CSP section 5.2.1.1)
7. Hard Copy Media Protection – User shall create and keep current a policy describing the procedures used to secure media hard copy criminal history results from unauthorized access/disclosure. The policy shall include, but not be limited to, destruction of paper media prior to further disposal, i.e., shredding before recycling. (CSP section 5.8) If User contracts with a third party company for the destruction of criminal history information, the destruction shall be witnessed by authorized User personnel. If the User stores hard copy media with a third party company, the media shall be secured in a way that access/view to the criminal history information is protected.
8. Controlled Area – User shall designate appropriate areas for accessing, processing, and storing criminal history information. Access to such areas shall be limited to authorized personnel only, during access/processing. Electronic data stored should meet FIPS 197/AES 256 standards and transmitted data should meet FIPS 140-2 requirements. Access to the application used to process/store criminal history information from outside the User shall include advanced authentication. (CSP section 5.9.2)
9. Formal Audits and Audit Record Retention – User may be audited at any time and will be audited at least triennially by FDLE to ensure compliance with this agreement. The audit may either be on-site at the User's location or via correspondence, at FDLE's discretion. (CSP section 5.11) The User may also be selected for FBI audits. (CSP section 5.4.6)

Revised 3/14/2018

Attachment # 1
Page 8 of 11

The User must retain audit records and dissemination logs for a minimum of at least one (1) year.

10. Personnel Security – FDLE has determined that Florida Statutes do not require the User to conduct state and national fingerprint based records check for non-criminal justice access to criminal history information. Therefore, compliance with these provisions does not require criminal history record checks of persons who access records. (CSP section 5.12)
11. Incident Response – User shall establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities and create and keep current a policy that defines the response procedures for a security incident, relating to any compromise of physical or electronic criminal history information. The procedures shall include notification to the CJIS Information Security Officer at CJISISO@FDLE.STATE.FL.US. (CSP section 5.3)

*Additional Requirements Applicable to Users Maintaining Criminal History Information
In Electronic Format*

12. Access Control/Encryption – The User shall ensure criminal history information is encrypted when transmitted or stored outside the User facility. Encryption shall meet the FIPS 140-2 standard. (CSP section 5.5.2.4)
13. Logging – The User shall retain system generated audit logs from any system that is used to store, transmit, or process criminal history information (either from the application and/or operating system level) for at least 365 days to ensure conformance to prescribed security and access requirements.
14. Electronic Media Protection – User shall create and keep current a policy describing the procedures used to secure electronic media criminal history results from unauthorized access/disclosure. The policy shall include, but not be limited to, destruction of electronic media prior to further disposal, i.e., wiping a hard drive before disposing or returning to a vendor. (CSP section 5.8) If User contracts with a third party company for the destruction of criminal history information, the destruction shall be witnessed by authorized User personnel.
15. Identification and Authentication – User shall ensure access to systems used to process/store criminal history information requires individual authentication to verify that a user is authorized access to criminal history information. Passwords shall meet required security standards (CSP section 5.6.2.1). Advanced authentication shall be used for access originating from any controlled area. (refer to CSP section 5.6)
16. Configuration Management – User shall maintain a network topological diagram depicting the system and network used to process or store criminal history information, and shall provide the diagram to FDLE/FBI during the audit process. (CSP section 5.7)

Revised 3/14/2018

Attachment # 1
Page 9 of 11

17. System and Communications Protection and Information Integrity – User shall implement the proper safeguards to ensure the confidentiality and integrity of criminal history information, to include, but not be limited to:

- a. Encryption of data during transmission and at rest
- b. Implementation of firewalls
- c. Use of intrusion detection tools
- d. Use of separate Virtual Local Area Network for voice over internet protocol
- e. Adhering to proper patch management
- f. Use of software to detect and eliminate malware, spam, spyware. (CSP section 5.10)

V. Termination

Either FDLE or User may suspend the performance of services under this agreement when, in the reasonable estimation of FDLE or User, the other party has breached any material term of the agreement. Furthermore, upon FDLE becoming aware of a violation of this agreement which might jeopardize Florida's access to federal criminal history information, FDLE shall have the option of suspending services under this agreement, pending resolution of the problem. The violation of any material term of this agreement or of any substantive requirement or limitation imposed by the federal or state statutes, regulations, or rules referred to in this agreement shall be deemed a breach of a material term of the agreement.

Section 943.053(4), F.S., provides that criminal history record information received from FDLE "shall be used only for the purpose stated in the request." National criminal history information received from the FBI is made confidential by federal law and regulation. Section 815.04(3)(b), F.S., prohibits, as a third-degree felony, the willful and knowing disclosure of data from a computer system, without authorization, which data is made confidential by law.

VI. Miscellaneous

A. User agrees that:

1. User is currently operating a lawful business or other entity within the state of Florida, with a physical address in Florida.
2. User is legally authorized to operate its business or other entity within the state of Florida.
3. User has complied and will continue to comply with all requirements to properly operate its business or other entity within the state of Florida.

Revised 3/14/2018

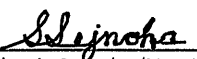
Attachment # 1
Page 10 of 11

4. User shall promptly notify FDLE upon any change to the above, including but not limited to name, address, and status as a business or other entity operating in Florida.
- B. This agreement supersedes any previous agreements concerning the NCPA of 1993, as amended, and/or Section 943.0542, F.S.
- C. This agreement may be amended by FDLE as needed, to comply with state or federal laws or regulations, or administrative needs of FDLE.
- D. This agreement is binding upon all User employees, agents, officers, representatives, volunteers, contractors, vendors, successors in interest, beneficiaries, subsidiaries, and assigns.

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

NAME OF USER ENTITY Palm Beach County Board of County Commissioners - Division of Consumer Affairs

ENTITY HEAD Stephanie Sejnoha **TITLE** Director Public Safety Department
(PLEASE PRINT)

ENTITY HEAD 
Stephanie Sejnoha (May 18, 2018)
(SIGNATURE)

DATE May 18, 2018

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY  **TITLE** OMCM
Ebony Tisby (May 18, 2018)

DATE May 18, 2018

Revised 3/14/2018

Attachment # 1

Page 11 of 11