COLUMBIA COUNTY BOARD OF COUNTY COMMISSIONERS
AGENDA ITEM REQUEST FORM

The Board of County Commissioners meets the 1st and 3rd Thursday of each month at 5:30 p.m. in the Columbia County School Board Administrative Complex Auditorium, 372 West Duval Street, Lake City, Florida 32055. All agenda items are due in the Board's office one week prior to the meeting date.

Today's Date: 7/7/2020 **Meeting Date:** 7/16/2020

Name: John Crews **Department:** BCC Administration

Division Manager's Signature: Ben Scott

1. Nature and purpose of agenda item:

The attached agreement allows the human resource department to request fingerprint background checks for volunteers and employees through FDLE.

2. Recommended Motion/Action:

Approve and sign the acknowledge receipt of the Volunteer & Employee Criminal History System Handbook and the VECHS Agreement

3. Fiscal impact on current budget.

This item has no effect on the current budget.

VECHS Handbook

For Qualified Entities

Volunteer Employee Criminal History System

National Child Protection Act of 1993, as amended,
and Section 943.0542, Florida Statutes

VECHS Contact Information

Mailing Address

FDLE
User Services Bureau/VECHS
PO Box 1489
Tallahassee, Florida 32302-1489

Physical Address

FDLE
User Services Bureau/VECHS
2331 Phillips Road
Tallahassee, Florida 32308

Direct Contact

Phone Number: (850) 410-8161
Fax Number: (850) 488-4424
Email: PublicRecords_VECHS@fdle.state.fl.us

Hours of Operation

Monday – Friday
8:00 a.m. – 5:00 p.m.

Other Resources

FDLE Home: www.fdle.state.fl.us
CHS Home: www.fdle.state.fl.us/Criminal-History-Records/Obtaining-Criminal-History-Information.aspx
VECHS Home: www.fdle.state.fl.us/Background-Checks/VECHS-Home.aspx

Table of Contents

Welcome to Florida's VECHS Program

Welcome to the VECHS Program at the Florida Department of Law Enforcement (FDLE). We appreciate your participation in the VECHS Program, and your goal to protect children, the elderly, and the disabled. We look forward to providing you with state and national criminal history record checks, in conjunction with the Federal Bureau of Investigation (FBI), on your current and/or prospective employees (E) and/or volunteers (V), through your submission of electronic fingerprints, pursuant to the National Child Protection Act of 1993, as amended, and section 943.0542, Florida Statutes (1999).

Please visit the VECHS website at http://www.fdle.state.fl.us/Background-Checks/VECHS-Home.aspx for more information about the program, forms, and frequently asked questions.

VECHS Overview

VECHS (pronounced "vecks") is an acronym for the Volunteer & Employee Criminal History System at the Florida Department of Law Enforcement (FDLE). The VECHS program was implemented in 1999 and is authorized by the National Child Protection Act (NCPA) (1993), as amended, and Florida Statute 943.0542 (1999). The mission of the program is to protect children, the elderly, and the disabled.

Through the VECHS program, FDLE and the Federal Bureau of Investigation (FBI) provide state and national criminal history record information on applicants, employees, and volunteers to qualified organizations (not individuals) in Florida. With this criminal history information, the organizations can more effectively screen out those current and prospective volunteers and employees who are not suitable for contact with children, the elderly, or the disabled.

To be qualified to participate in the VECHS program, an organization (public, private, profit, or non-profit) must offer "care" or "care placement services," or facilitate a program that offers "care" or "care placement services," as defined in the above laws, exclusively to children, the elderly, or the disabled, even if such program is only a limited part of the organization's overall business.

The VECHS program is not available to organizations that are otherwise statutorily required to obtain criminal history record checks on their employees and/or volunteers, such as daycare centers. Those organizations must continue to follow the statutory mandates that specifically apply to them. If, however, an organization is required to obtain state and national checks on only specific types of employees or volunteers, the VECHS program may be able to process requests for state and national checks on the organization's other employees or volunteers.

Participation in the VECHS program is strictly voluntary for those organizations that are not statutorily required to obtain criminal history record checks on their employees and volunteers. The National Child Protection Act (NCPA) does **not** replace the existing Florida statutes that mandate state and national criminal history record checks for employees of specified caretaker programs, which include, but are not limited to the following: school district instructional and non-instructional personnel, nursing home administrators and financial officers, and child care, substance abuse, mental health, and developmental service programs. If your organization is presently required to obtain criminal history checks on employees and/or volunteers, you must continue to do so under the applicable Florida law.

VECHS Overview, (continued)

Once an organization becomes qualified and provides the required information for criminal history record requests, FDLE, with the assistance of the FBI, will provide the organization with the following:

- An indication that the person has no criminal history, i.e., no serious arrests in state or national databases, if there are none;
- The criminal history record (RAP sheet) that shows arrests and/or convictions for Florida and other states, if any;
- Notifications of any warrants or domestic violence injunctions that the person may have.

The qualified entity will need to review the information to determine if there is any reason that the employee or volunteer should not be allowed to work with children, the elderly, or the disabled. If no criminal history record is found, an entity should not necessarily assume that there are no risks to employing or using the volunteer services of the individual. Simply stated, "no record" means that he or she does not have an arrest or conviction known to FDLE or the FBI.

If the employee or volunteer has a criminal record, the qualified entity should evaluate whether the individual should be permitted contact with children, the elderly, or the disabled. Neither the NCPA nor Florida law governing the VECHS program defines specific criteria to use during this evaluation of an entity's employee or volunteer. Therefore, FDLE does not set specific screening criteria either.

VECHS Waiver Form

Obtain a completed and signed VECHS Waiver Agreement and Statement or VECHS Private School Waiver Agreement and Statement from every current or prospective employee and volunteer for whom the qualified entity submits a request for a criminal history record check to FDLE. The signed waiver form allows the release of state and national criminal history record information to the qualified entity.

Original waiver forms must be retained by the qualified entity for as long as the employee or volunteer is working or for five years, whichever is longer.

Personal Review

Florida and federal laws afford individuals the right to request a copy of their criminal history record for purposes of personal review, to ensure that it is accurate and complete. The requester may examine the record and challenge any inaccurate or incomplete information. There is no charge assessed by FDLE for this service.

More information can be found at the following website:

http://www.fdle.state.fl.us/Criminal-History-Records/Personal-Review.aspx

If you have any questions about this process, please contact the Criminal History Record Maintenance section at (850) 410-7898.

Electronic Submissions

Criminal history record checks are one of several methods of determining the suitability of individuals who seek employment or volunteer positions with organizations. The NCPA specifies that the criminal history records search must be based upon fingerprints. Therefore, each request for a criminal history background search must be accompanied by a set of 10-print fingerprints.

Criminal history record check requests are processed through the Civil Workflow Control System (CWCS), pronounced "QUICKS", an automated system used to receive, process and respond to electronic requests for applicant criminal history record checks. These checks are completed within 24-72 hours after receipt of the transaction and the results are posted to a secure mail application.

The cost of each electronically submitted record request will be **$37.25** for employees and **$29.25** for volunteers, and is set by state and national laws. All "service providers" will assess a fee in addition to the cost of the actual criminal history for capturing the fingerprints and submitting them to FDLE. A list of registered service providers can be found on the VECHS website.

Criminal history results for electronic submissions are posted to FDLE's secure mail application, SecureMail. Once the criminal history results are ready, your entity will receive an e-mail notification containing a link to the application where criminal history results may be viewed.

Rejected Fingerprints

Electronic images may be rejected for various reasons; for example, fingerprints that do not have legible patterns will be rejected by the FBI. A rejection notice will be returned to the submitting entity along with the state of Florida results via SecureMail. A new set of fingerprints along with the transaction control reference number (TCR) must be resubmitted electronically for proper processing. The TCR can be found in the rejection notice from the FBI. This number is unique, can only be used once, and is specifically tied to the transaction control number (TCN) for the fingerprinted applicant.

All resubmissions must be returned within 180 days from the date the original fingerprint submission was rejected. New fees will be assessed for resubmissions of fingerprints that do not include the TCR number or are not resubmitted within 180 days. If fingerprints are rejected a second time after providing fingerprints with the TCR number, a name search is to be requested of the FBI (see next section: Name Searches).

Name Searches

The FBI will conduct a name-based search for individuals whose fingerprints are rejected based on image quality for two separate sets of fingerprints. A duplicate image cannot be submitted; two different sets of images must be submitted and subsequently rejected for the FBI to conduct a name search. The entity must complete a CJIS Name Search Request Form and either fax or mail the form directly to the FBI. All requests for name-based searches must be submitted within 90 days of the second rejected transaction notice.

On the name check form, the "ORI of State/Federal/Regulatory Agency" and "Address of requesting agency" have already been populated with the appropriate data and should not be modified. VECHS customers may choose to either fax the completed CJIS Name Search Request Form to (304) 625-5102 (ATTENTION: NAME CHECK REQUEST) or submit the form via mail to the following address:

FBI CJIS DIVISION
IDENTIFICATION AND INVESTIGATIVE SERVICES SECTION
MODULE E-2
1000 CUSTER HOLLOW ROAD
CLARKSBURG, WV 26306
ATTENTION: NAME CHECK REQUEST

Please remember that all requests for name-based searches must be submitted within 90 days of the second rejected fingerprint notice. Please be sure to complete the contact and phone/fax number information for your entity. To ensure complete and accurate processing, please also include your assigned entity number in the "Entity/OCA Number" field at the bottom of the form.

Applicant Fingerprint Retention Notification Program (AFRNP)

FDLE developed the Arrest Fingerprint Retention Notification Program (AFRNP) because of legislative mandates for the retention of certain electronically submitted applicant fingerprints and monitoring for new arrests. All incoming Florida arrest fingerprints are searched against fingerprints retained in the AFRNP. When the subject of retained fingerprints is identified with fingerprints of an incoming Florida arrest, FDLE notifies the submitting agency of the arrest (referred to as an arrest hit notification). The arrest hit notifications will include the name of the arresting agency.

The AFRNP can only conduct searches against incoming Florida arrest fingerprints. Arrests made in other states or by the federal government will NOT result in arrest hit notifications. Information on arrests in other states or the federal government is only available in the results of a state and national criminal history record check.

The quality of fingerprints submitted into the AFRNP has a direct effect on the search and the resulting arrest hit notification. Customers should understand if submitted fingerprints for an applicant or an arrested individual were of sub-standard quality, the identification of the applicant as the arrested person may not occur and an arrest notification may not be made. Also, until the arrest fingerprint submission is actually received by FDLE, there is no way to identify an arrested person as an individual retained in the AFRNP.

IMPORTANT NOTE

FDLE retains only those applicant fingerprints authorized by law. All other applicant fingerprints submitted ARE NOT automatically retained in the AFRNP. An entity may request retention of fingerprints in the AFRNP by submitting this request in writing on agency letterhead.

Retained Fingerprint Invoices and Fees

The cost for the first year of fingerprint retention is included in the initial background check fee. After the first year of retention, the annual fee for participation in the AFRNP is $6.00 per individual record retained. Entities will be billed for this fee annually based upon the anniversary month of the initial fingerprint record retention date.

IMPORTANT NOTE

FDLE retains only those applicant fingerprints authorized by law. All other applicant fingerprints submitted ARE NOT automatically retained in the AFRNP. An entity may request retention of fingerprints in the AFRNP by submitting this request in writing on agency letterhead.

Retaining fingerprints allows your entity the ability to do the following:

1. Request a rescreening on any set of retained fingerprints for the cost of $13.25 per employee resubmission, or $11.25 per volunteer resubmission.
2. Receive Florida arrest hit notifications for those associated employees and/or volunteers.

If you wish to participate in the retention notification program, you will need to e-mail your request and include the following information:

- The VECHS qualified entity number(s) that you wish to retain fingerprints for (indicate employee only, volunteer only, or both);
- Your acknowledgment that you are required to pay an annual retention fee of $6.00 for each set of retained prints;
- A statement that you understand that any previously submitted transactions will not be retained; and
- An effective date that you would like FDLE to start retaining the fingerprints (at least 2 weeks from the date of your email)

If you wish to retain your applicant fingerprints, please e-mail your request to PublicRecords_VECHS@fdle.state.fl.us.

Reminders

All records obtained through this program must be stored in a secure area and apart from other documents.

VECHS program records are subject to audit by state and federal government officials.

Criminal history information may only be used for screening purposes that are defined in your user agreement.

Criminal history information or records may not be shared with other persons, companies, agencies, or entities, except as authorized by your user agreement and the laws governing this program.

Record information may only be shared with other qualified VECHS entities **after** confirming with FDLE the status of the entity. In addition, a secondary dissemination log (VECHS Dissemination Log) must be maintained detailing the facts about what, when, where and to whom any information is shared. All record information should be retained for a minimum of five years or for as long as the employee/volunteer is active with your entity, whichever is longer.

Notify the Criminal History Services Section with the VECHS Account Update Form whenever there are changes to your entity name, entity head, physical and/or operating address, mailing address, contact person, phone numbers, or any other information that may affect your user agreement with FDLE.

FDLE retains only those applicant fingerprints authorized by law. All other applicant fingerprints submitted ARE NOT automatically retained in the AFRNP. An entity may request retention of fingerprints in the AFRNP through the process listed on Page 11 .

FDLE
Florida Department of
Law Enforcement

VECHS
Volunteer and Employee
Criminal History System

VECHS Handbook Acknowledgement Form

This form requires VECHS entities to acknowledge receipt of the VECHS Handbook, attached hereto. Representatives or employees of the VECHS entity are encouraged to contact the Florida Department of Law Enforcement (FDLE) in the event the entity has questions regarding any of the policies, procedures, or forms discussed in this handbook.

For inquiries related to the VECHS program, VECHS Handbook, policies, or associated forms, please contact FDLE at:

(850) 410-8161
PublicRecords_VECHS@fdle.state.fl.us

Entity Name

Entity Head

Entity Head Title

Entity Head Signature

Date

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 COLUMBIA COUNTY BOARD OF COUNTY COMMISSIONERS with entity number: E/V12020002 (hereinafter referred to as User), located at 135 NE HERNANDO AVE. LAKE CITY, FL 32055 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.

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.

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.

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

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

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.

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.

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)

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)

17. System and Communications Protection and Information Integrity – User shall implement the proper safeguards to ensure the confidentially 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.

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 COLUMBIA COUNTY BOARD OF COUNTY COMMISSIONERS

ENTITY HEAD_____ **TITLE**_____
(PLEASE PRINT)

ENTITY HEAD_____
(SIGNATURE)

DATE_____

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY_____ **TITLE** Operations and Management Consultant Manager

DATE_____