

SUPERIOR COURT OF CALIFORNIA  
SANTA CLARA COUNTY  
JUVENILE COURT DIVISION  
STANDING ORDER

**FILED**  
FEB 02 2023  
Clerk of the Court  
Superior Court of Santa Clara County  
BY CATHERINE ADAMS DEPUTY

**AUTHORIZATION FOR THE COUNTY OF SANTA CLARA PROBATION  
DEPARTMENT TO ACCESS AND SHARE JUVENILE CASE FILES WITH SAN JOSÉ  
STATE UNIVERSITY RESEARCH FOUNDATION**

San José State University Research Foundation (SJSU) and the National Center for Youth Law (NCYL) collaborate to jointly provide the Justice Education (“Justice Ed”) Program to youth supervised by the County of Santa Clara Probation Department. The overarching goal of the Justice Ed Program is to improve education outcomes and reduce recidivism rates for all youth experiencing formal probation supervision in Santa Clara County. SJSU and NCYL, through the Justice Ed Program, facilitate strong regional cross-system partnerships between multiple agencies and organizations to help youth attain their educational goals.

SJSU seeks to evaluate the impact of the Justice Ed Program on recidivism outcomes for juvenile justice-involved youth in Santa Clara County. Because SJSU plans to study a particular juvenile justice population for purposes of discerning the impact of the Justice Ed Program on youth, Welfare and Institutions Code section 827.12 authorizes the Juvenile Court to permit the Probation Department to access and share its juvenile case files with SJSU if the Juvenile Court makes the required findings in Section 827.12 regarding confidentiality protections and redisclosure safeguards.

After reviewing the attached Agreement between SJSU and the County (a true and correct executed copy of which is attached as Exhibit A and incorporated herein), the Juvenile Court finds that SJSU’s study will include:

- (1) a sound methodology for protecting the confidentiality of juvenile case files that will be accessed; and
- (2) procedures to prevent the redisclosure of personally identifying information from the files.

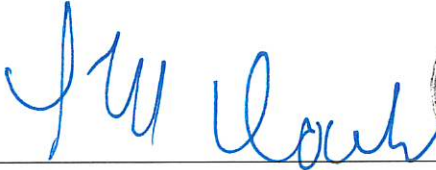

Therefore, pursuant to its authority under Section 827.12 of the Welfare and Institutions Code and based on its findings regarding confidentiality and redisclosure, the Juvenile Court authorizes the Probation Department to access and disclose juvenile case files of the youth identified by SJSU. SJSU’s access is contingent upon compliance with all terms of the Agreement between SJSU and the County.

//

//

During the course of this study, all personally identifying information with respect to any youth whose records are disclosed pursuant to this Standing Order shall be fully and appropriately redacted prior to any public discussions or presentations in accordance with all applicable laws. All data collected from the County pursuant to this Standing Order shall be destroyed as required by the terms of the Agreement between SJSU and the Probation Department.

SO ORDERED:

---

The Honorable L. Michael Clark  
Presiding Judge of the Juvenile Division

Dated: 2-2-2023

**DATA USE AGREEMENT BETWEEN THE COUNTY OF SANTA CLARA AND SAN JOSÉ STATE  
UNIVERSITY RESEARCH FOUNDATION**

This Data Use Agreement (“Agreement”) is entered into by and among San José State University Research Foundation (“SJSU” or “Research Entity”) and the County of Santa Clara (“County”) (together the “Parties,” and each a “Party”) to govern the sharing of juvenile case file information by the County of Santa Clara Probation Department (“Probation Department”).

**WHEREAS**, SJSU, in partnership with the National Center for Youth Law (NCYL), provides the Justice Education (“Justice Ed”) Program, which affords educational support to juvenile justice involved youth supervised by the Probation Department, to help such youth attain their educational goals, improve educational outcomes, and reduce recidivism rates;

**WHEREAS**, SJSU seeks to evaluate the Justice Ed Program to determine its impact on participants by analyzing juvenile justice data that is maintained by the Probation Department;

**WHEREAS**, the Probation Department maintains juvenile case files regarding the juvenile justice involvement of youth;

**WHEREAS**, the Parties share the goals of improving outcomes for juvenile justice involved youth and all youth;

**WHEREAS**, the Juvenile Division of the Superior Court, State of California, County of Santa Clara (“Juvenile Court”), under California Welfare and Institutions Code Section 827.12, may authorize the Probation Department to access and provide juvenile case file information for data sharing on a juvenile justice population or practice if the proposed study meets the confidentiality requirements in Section 827.12; and

**WHEREAS**, the Juvenile Court found that the study proposed by the Research Entity would meet Section 827.12’s confidentiality requirements if this Agreement is entered into by the Parties.

**NOW, THEREFORE**, the Parties agree as follows:

**I. TERM OF AGREEMENT**

The Agreement shall be effective upon execution by the Parties. The Agreement shall remain in effect until completion of the Research Project (as defined below) or until five years from the date of the execution of the Agreement, whichever is earliest, unless earlier terminated by one of the Parties pursuant to Section VII.B., “Termination.”

**II. PURPOSE AND BACKGROUND**

**I. Research Project Description.** Research Entity is requesting data from the Probation Department regarding youth referred to any educational program (e.g., Justice Ed, Project YEA, and LACY) from January 2017 to June 2022, to evaluate the impact of educational support

received by Justice Ed Program participants on recidivism rates as compared to other justice involved youth that receive educational support from different educational programs. The data requested is part of phase one of the Justice Ed Program evaluation, which is aimed at identifying a comparison group of youth by analyzing a sample of youth supervised by the Probation Department to determine a profile of risk factors, needs, and recidivism outcomes for youth currently referred to educational support programs (the “Research Project”).

**II. Research Project Deliverables.** Research Entity will conduct latent class analysis—a data reduction process that uses variables to determine classes of risk factors to categorize youth needs. Research Entity will complete a report that includes narrative profiles and descriptive statistics of each risk class and provide the report to the Probation Department and NCYL. NCYL will include the findings from the report in its Year 3 Justice Ed Program evaluation report, which will be published on NCYL’s website and shared with the Probation Department and other County partners.

### **III. CONFIDENTIALITY AND AUTHORITY TO DISCLOSE JUVENILE CASE FILE INFORMATION TO RESEARCH ENTITY**

**A. Information Requested.** Upon execution of this Agreement, the Probation Department will provide Authorized Staff (as defined below in Section IV.B) from Research Entity with access to juvenile case file information (as identified in Appendix A, which is attached and incorporated herein) for the youth populations identified by the Research Entity (“Juvenile Case File Information”). Juvenile Case File Information does not include dependency information contained in the juvenile case files maintained by the Probation Department. Research Entity may use the Juvenile Case File Information only for the purposes set forth in this Agreement and will only access the minimum information necessary to conduct the Research Project (as defined above). Research Entity shall not redisclose Juvenile Case File Information to any person or entity not specifically authorized by this Agreement to receive it.

**B. Ownership.** The County retains ownership of the Juvenile Case File Information and hereby grants Research Entity a worldwide, royalty-free, non-transferable, non-exclusive license to use Juvenile Case File Information solely for the purposes outlined in this Agreement; Research Entity does not claim any right, title, or ownership of Juvenile Case File Information, or a license to use Juvenile Case File Information for any other purpose.

**C. Juvenile Case File Information.** The Parties acknowledge that Welfare and Institutions Code Section 827 generally prohibits the disclosure of information contained in juvenile case files with limited exceptions for individuals entitled to access under Section 827 or another section of the Welfare and Institutions Code.

The Parties further acknowledge that Welfare and Institutions Code Section 827.12 permits the Probation Department to access and disclose Juvenile Case File Information to authorized individuals for the purpose of conducting or facilitating research on particular juvenile justice system populations or practices if the Juvenile Court authorizes the Probation Department to share juvenile case files with those authorized individuals after making the confidentiality-related findings in Section 827.12(a)(2).

The Parties further acknowledge that Research Entity is requesting access to Juvenile Case File Information for purposes that relate to particular juvenile justice system populations and practices: evaluating the impact of the Justice Ed program on youth participants' recidivism rates.

The Parties further acknowledge that the Juvenile Court may authorize the Probation Department to access and provide Juvenile Case File Information to Research Entity for this purpose if the confidentiality and redisclosure requirements in Welfare and Institutions Code Section 827.12 are met. After reviewing this Agreement, the Juvenile Court authorized the Probation Department to disclose Juvenile Case File Information to Research Entity in its Standing Order regarding authorization for the County of Santa Clara Probation Department to access and share juvenile case files.

The Parties acknowledge and agree that the Juvenile Court's authorization to access Juvenile Case File Information is contingent upon their execution of and compliance with this Agreement.

**D. Juvenile Case File Information Access.** The Probation Department will transmit Juvenile Case File Information to Research Entity via secure means approved by the County Information Security Office. The Juvenile Case File Information will encompass youth referred to any educational program (*e.g.*, Justice Ed, Project YEA, and LACY) from January, 2017 to June, 2022.

**E. Data Masking Protocol.** If the Juvenile Case File Information includes any personally identifying information (PII), as defined in subdivision (b) of Civil Code section 1798.79.8, the County will "mask" the PII—meaning that any PII will be replaced with structurally similar, fake data—before transmitting the Juvenile Case File Information to the Research Entity. The County will primarily utilize the substitution and date aging methods to mask the PII in the Juvenile Case File Information.

**F. Redisclosure of Personally Identifying Information Prohibited.** Research Entity shall not redisclose any personally identifying information (as defined in Civil Code Section 1798.79.8(b)) in any public report or presentation or to any person not specifically authorized by this Agreement to receive that information.

**G. Juvenile Case File Information Use and Publication.** Research Entity may use Juvenile Case File Information only as authorized under the terms of this Agreement and only to execute the Research Project and produce the Research Project Deliverables identified in Section II. Before Research Entity publishes or otherwise publicly releases any anonymized Juvenile Case File Information or information or data derived therefrom, the Probation Department must have the opportunity to review prior to their publication and release.

#### **IV. ACCESS TO JUVENILE CASE FILE INFORMATION BY AUTHORIZED STAFF**

**A. Staff Oversight.** Research Entity shall ensure that all staff involved in the

Research Project adhere to the requirements for confidentiality, disclosure, transmission, destruction, storage of, and access to Juvenile Case File Information described in this Agreement.

**B. Authorized Staff.** Research Entity shall limit—as much as possible without impeding the Research Entity’s work and processes—the number of staff required to access Juvenile Case File Information to accomplish the Research Project. The following Research Entity staff member(s) (“Authorized Staff”) will have access to Juvenile Case File Information:

Staff member name: Edward Cohen, Ph.D.

Qualifications (e.g., education and related training):

Dr. Cohen has had extensive training in the protection of human subjects data and the conduct of ethical research on human subjects. He has also managed several grant-funded projects that required Institutional Review Board (IRB) approval and oversight. As required by the university IRB, Dr. Cohen completed the online Collaborative Institutional Training Initiative (CITI) course on research with human subjects in December, 2021. A copy of the certificate is available upon request.

Before allowing any staff member not identified above to access Juvenile Case File Information, Research Entity must receive the Probation Department’s written approval. Each member of the Authorized Staff will be assigned a unique user name and password to access Juvenile Case File Information, which must be kept confidential. Sharing of user names and passwords by Authorized Staff is prohibited. To the extent required under this Agreement or by a County entity reviewing the research request, Authorized Staff will submit to a background check. Research Entity shall also inform the County within two business days after an Authorized Staff member ceases working on the Research Project, with a written assurance that the staff member’s access to all Juvenile Case File Information has been removed and a description of the reason for the staffing change.

**C. Passwords.** Passwords to access the Research Entity’s systems storing Juvenile Case File Information must comply with the Strong Password requirements set forth in Appendix B.

**D. Training.** Research Entity will instruct all members of the Authorized Staff about the requirements for handling Juvenile Case File Information and about the potential sanctions for unauthorized disclosure or use of Juvenile Case File Information. Research Entity will ensure that Authorized Staff have been informed of the mandatory procedures for maintaining the confidentiality of Juvenile Case Information and that unauthorized dissemination or use thereof could lead to civil and criminal penalties.

## **V. SECURE TRANSMISSION, STORAGE, AND ANALYSIS OF DATA**

**A. Transmission.** All Juvenile Case File Information will be shared via secure file sharing protocols approved by the County Information Security Office. Research Entity will not have direct access, remote or otherwise, to any County data system.

**B. Secure Storage of Juvenile Case File Information by Research Entity.** All Juvenile Case File Information transferred to Research Entity shall be stored in a password protected computer and not copied or shared via any cloud-based platform or program, located at 1 Washington Square, Room 216, San José, California 95192. Research Entity must comply with the County's Security Addendum attached as Appendix B. If Juvenile Case File Information will be accessible remotely, Research Entity must notify the County and must only allow access to Juvenile Case File Information via a secure Virtual Private Network (VPN). Under no circumstances shall Juvenile Case File Information be hosted in the cloud. Only Authorized Staff shall have access to Juvenile Case File Information. Authorized Staff shall only print documents when reasonably necessary to carry out the Research Project. Documents containing Juvenile Case File Information must not be left unattended. All printed documents must be stored in a locked and secured location that can only be accessed by Authorized Staff. If possible, Research Entity will store documents in locked desks or cabinets.

**C. Audits, Inspection, and Enforcement.** Within ten days of a written request from the County, Research Entity shall allow the County to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies, and/or procedures relating to the use or disclosure of Juvenile Case File Information pursuant to this Agreement for the purpose of determining whether Research Entity is in compliance with this Agreement's terms. Research Entity and the County shall mutually agree in advance upon the scope, timing, and location of such an inspection. The County shall protect the confidentiality of any confidential and proprietary Research Entity information to which it has access during the inspection, and shall execute a nondisclosure agreement, upon terms mutually agreed upon by the Parties, if requested by Research Entity.

The fact that the County inspects, or fails to inspect, or has the right to inspect, Research Entity's facilities, systems, books, records, agreements, policies, and/or procedures does not relieve Research Entity of responsibility to comply with this Agreement, nor does the County's (i) failure to detect, or (ii) detection, but failure to notify Research Entity or require Research Entity's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of the County's rights under this Agreement.

**D. Security Incidents.** Research Entity must report to the County in writing any use, modification, or disclosure related to a Research Entity system storing Juvenile Case File Information of which it becomes aware immediately after discovery. Research Entity must report to the County in writing any access to, use, modification, or disclosure of Juvenile Case File Information not permitted by this Agreement of which it becomes aware immediately after discovery. The County has the right to investigate or decline to investigate any report of unauthorized use. Research Entity shall comply with all County investigations and comply with all data breach response obligations. The County has the right to suspend or terminate Research Entity's use of Juvenile Case File Information for any security incident, and to reinstate access only after satisfactory assurances have been provided to the County.

The written security incident notice must be provided to the Chief Information Security Officer, County Counsel's Office, and Probation Department Deputy Director of Probation



Administration and contain: (1) a brief description of what happened, including the date of the Security Incident and the date of the discovery; (2) the location of the security incident; (3) a description of the types of Juvenile Case File Information that were involved in the security incident; (4) safeguards in place prior to the security incident; (5) actions taken in response to the security incident; and (6) a brief description of what Research Entity is doing to investigate the security incident, to mitigate harm to individuals, and to protect against further security incidents.

Information Security Office  
Justin Dietrich, Chief Information Security Officer  
2460 North First Street, Suite 220  
San José, CA 95131  
[justin.dietrich@iso.sccgov.org](mailto:justin.dietrich@iso.sccgov.org)

Office of the County Counsel  
Marcelo Quiñones, Lead Deputy County Counsel  
70 West Hedding Street, East Wing, Ninth Floor  
San José, CA 95110  
[marcelo.quinones@cco.sccgov.org](mailto:marcelo.quinones@cco.sccgov.org)

Probation Department  
Mariel Caballero, Deputy Director of Probation Administration  
2314 North First Street  
San José, CA 95131  
[Mariel.Caballero@pro.sccgov.org](mailto:Mariel.Caballero@pro.sccgov.org)

Should Juvenile Case File Information be divulged to unauthorized third parties, Research Entity shall comply with all applicable federal and state laws and regulations, including, but not limited to, California Civil Code sections 1798.29 and 1798.82 at Research Entity's sole expense. Research Entity shall not charge County for any expenses associated with Research Entity's compliance with these obligations.

## **VI. DESTRUCTION OF DATA**

**A.** Research Entity may retain Juvenile Case File Information until five years from the date this Agreement is executed. After five years from the date of execution, Research Entity shall destroy all Juvenile Case File Information in its possession.

**B.** In the event of an early termination of this Agreement pursuant to Section VII.B, Research Entity will destroy all Juvenile Case File Information in its possession as soon as commercially practicable.

**C.** Research Entity shall use any method of confidential destruction meeting industry standards, including shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using industry standard destruction software for electronic file destruction.



**D.** Research Entity will provide the County with a Certificate of Destruction of Juvenile Case File Information that identifies the method of destruction within 14 days of when the destruction of Juvenile Case File Information occurs under Section VI.A or VI.B. Research Entity shall include the following information in the Certificate of Destruction:

- Listing of personnel who reviewed and approved sanitization and disposal actions;
- Types of media sanitized or destroyed;
- Specific files stored on the media;
- Sanitization/Destruction methods used;
- Date and time of the Sanitization actions;
- Personnel who performed the sanitization;
- Verification actions taken;
- Personnel who performed the verification; and
- Disposal action taken.

## **VII. GENERAL PROVISIONS, TERMINATION, REMEDIES, AND GOVERNING LAW**

**A. Entire Agreement.** This Agreement supersedes any prior oral or written understanding or communications between the Parties and constitutes the entire agreement of the Parties with respect to the subject matter hereto. This Agreement may not be amended or modified, nor any of its provisions waived, except in a written document signed by an authorized representative of the Parties.

**B. Termination.** Any Party may terminate this Agreement for any reason by providing the other Party with at least 30 days' prior written notice of such termination. Upon termination of the Agreement, the County shall have no further obligation to provide Juvenile Case File Information to Research Entity pursuant to this Agreement and Research Entity shall not use Juvenile Case File Information for any purpose and shall not release, publicize, or present any deliverables based on Juvenile Case File Information without the express written consent of the County.

**C. Assignment of Rights.** No Party may assign its rights under this Agreement without the express written permission of the other Party. Any assignment that does not comply with this provision will be deemed null and void.

**D. Notice.** Notice may be provided via electronic mail with confirmation of delivery or via certified mail to each Party at:

**County of Santa Clara:**  
Mariel Caballero  
Deputy Director of Probation Administration  
County of Santa Clara Probation Department  
2314 North First Street

San José, CA 95131  
[Marisel.Caballero@pro.sccgov.org](mailto:Marisel.Caballero@pro.sccgov.org)

**Research Entity:**

Deborah Maloney  
San José State University Research Foundation  
210 N. 4<sup>th</sup> St, 3<sup>rd</sup> Floor  
San José, CA 95112  
408 924 1421  
[deborah.maloney@sjsu.edu](mailto:deborah.maloney@sjsu.edu)

**E. Indemnification.** In lieu of and notwithstanding the pro rata risk allocation which might otherwise be imposed between the Parties pursuant to Government Code Section 895.6, the Parties agree that all losses or liabilities incurred by a Party shall not be shared pro rata but, instead, County and Research Entity agree that, pursuant to Government Code Section 895.4, each of the Parties hereto shall fully indemnify and hold each of the other Parties, their officers, board members, employees, and agents, harmless from any claim, expense or cost, damage or liability imposed for injury (as defined in Government Code Section 810.8) occurring by reason of the negligent acts or omissions or willful misconduct of the indemnifying party, its officers, employees or agents, under or in connection with or arising out of any work, authority or jurisdiction delegated to such party under this Agreement. No party, nor any officer, board member or agent thereof shall be responsible for any damage or liability occurring by reason of the negligent acts or omissions or willful misconduct of the other Parties hereto, their officers, board members, employees, or agents, under or in connection with or arising out of any work authority or jurisdiction delegated to such other Parties under this Agreement.

**F. California Public Records Act.** The County is a public agency subject to the disclosure requirements of the California Public Records Act ("CPRA"). If Research Entity's proprietary information is contained in documents or information submitted to the County, and Research Entity claims that such information falls within one or more CPRA exemptions, it must clearly mark such information "CONFIDENTIAL AND PROPRIETARY," and identify the specific lines containing the information. In the event of a request for such information, the County will make best efforts to provide notice to Research Entity prior to disclosure. If Research Entity contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from a court of law in Santa Clara County before the County is required to respond to the CPRA request. If Research Entity fails to obtain such remedy within the time the County is required to respond to the CPRA request, the County may disclose the requested information. Research Entity further agrees that it shall defend, indemnify and hold the County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorney's fees) that may result from denial by the County of a CPRA request for information arising from any representation, or any action (or inaction), by Research Entity.

**G. Governing Law and Venue.** This Agreement shall be construed, performed, and enforced in accordance with the laws of the State of California, without giving effect to its principles or rules of conflict of laws to the extent such principles or rules would require or

permit the application of the laws of another jurisdiction. Proper venue for any legal action regarding this Agreement shall be vested exclusively in state or federal court in the County of Santa Clara. The Parties agree that subject matter and personal jurisdiction are proper in state or federal court in Santa Clara County. The Parties waive all venue and jurisdiction objections.

**H. Counterparts.** This Agreement may be executed in counterparts, each of which shall be deemed an original, and all of which, together, shall constitute one and the same instrument.

**I. Electronic Signatures.** The Parties agree that an electronic copy of a signed contract, or an electronically signed contract, has the same force and legal effect as a contract executed with an original ink signature. The term "electronic copy of a signed contract" refers to a transmission by facsimile, electronic mail, or other electronic means of a copy of an original signed contract in a portable document format. The term "electronically signed contract" means a contract that is executed by applying an electronic signature using technology approved by the County.

COUNTY OF SANTA CLARA

SAN JOSÉ STATE UNIVERSITY  
RESEARCH FOUNDATION

\_\_\_\_\_  
**Greta S. Hansen**                                  **Date**  
**Chief Operating Officer**

\_\_\_\_\_  
**Deborah Maloney**                                  **Date**  
**Director, Office of Sponsored Programs**

APPROVED

\_\_\_\_\_  
**Nick Birchard**    **Date**  
**Chief Probation Officer**

APPROVED AS TO FORM AND LEGALITY

\_\_\_\_\_  
**Mona M. Williams**                                  **Date**  
**Deputy County Counsel**

**Appendix A**  
**Juvenile Case File Information**

For the period of January, 2017, to June, 2022, the Probation Department will provide the following Juvenile Case File Information to Research Entity:

- (1) Offense history
  - a. WIC Offense(s) codes for youth offenses
  - b. Offense Type (felony vs. misdemeanor)
  - c. Offense Type (property vs. person)
  - d. Date of each offense
  - e. Date of Arrest
  - f. Petition Disposition
  - g. Age at first petition filing
- (2) JAIS risk
  - a. JAIS risk score
  - b. Supervision Strategies (all youth who have supervision strategies)
  - c. Interviewer Impression items (criminogenic needs) (all youth who have interviewer impressions)
- (3) Educational needs - JAIS
  - a. Did youth ever receive special education for learning deficiencies? (Q#10 on JAIS assessment)
  - b. Did youth ever receive special help for emotional or behavioral problems in school? (Q#11 on JAIS assessment)
  - c. Academic performance (Q #9)
  - d. School attendance (Q #13. Generally, do (did) you get your homework done?)
  - e. Relationship to school staff (Q #14 How do (did) you generally get along with your teachers and principals?)
  - f. School discipline (Q #15. Do (did) you have any other problems in school?)
  - g. Current school status (Q #16. Current school status)
  - h. Educational goal (Q #17. How far do you plan to go in school?)
- (4) Educational needs and other risks – Education Services Referral Form
  - a. Grade level
  - b. Whether or not Dually Involved Youth (Yes/No)
  - c. Primary reason for referral
  - d. Secondary reason for referral
  - e. Whether or not youth is open to Special Education Services (Yes/No)
  - f. Whether or not youth has mental health diagnosis (Yes/No)
  - g. Referral(s) made to educational support services – from Universal Referral Form – “Decision” and “Program Type”
  - h. Referral to Project YEA (yes or no, or other one-field indicator)
  - i. Referral to JusticeEd (yes or no, or other one-field indicator)
  - j. Referral to LACY (yes or no, or other one-field indicator)
- (5) Behavioral health risk factors - JAIS

- a. Youth substance use Q #22. A. How much drinking and/or drugs do you do?
  - b. Trauma exposure: Total number of traumas, 44a through 44j (or data can include specific items a-j)
- (6) Family risk factors - JAIS
- a. Parent history of criminal behavior Q #49b. Does any parent have a history of criminal behavior?
  - b. Parent history justice system involvement Q #49c. Does any parent have a history of probation, jail, or prison?
  - c. Parent emotional/psychiatric problems Q #49d. Does any parent have a history of psychiatric hospitalization?
  - d. Parent substance use: Q #49f. Does any parent have a history of drinking and/or drug problems?
- (7) Primary ethnicity of youth
- (8) Gender of youth
- (9) Age at JAIS assessment

## **Appendix B Security Addendum**

### **1. Information Security Management Program and Policies**

**1.1 Research Entity Security Contact.** Research Entity shall provide a security representative as a point of contact for County on any security issues.

**1.2 Policies and Procedures.** Research Entity shall maintain written security management policies and procedures to prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, and availability of Research Entity Processing Resources and/or Juvenile Case File Information. These policies and procedures shall:

- (a) assign specific data security responsibilities and accountabilities to specific individual(s);
- (b) include a risk management program that includes periodic risk assessments;
- (c) include a process to respond to the threats and vulnerabilities identified in the risk assessment to mitigate or remediate identified risks to an acceptable level; and
- (d) implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with federal, state, and local regulations.

**1.3 Infrastructure Protection.** Research Entity shall maintain policies and procedures to protect its Processing Resources, including:

- (a) security programs (policies, standards, processes, procedures, etc.);
- (b) processes for becoming aware of, and maintaining, security patches and fixes;
- (c) procedures for employing router filters, firewalls, and other mechanisms to restrict access to Research Entity Processing Resources, including all local-site networks that may be accessed via the Internet (whether or not such sites transmit information);
- (d) procedures for ensuring that resources used for mobile access have technology installed that is designed to protect against attack, penetration, and compromise (e.g. firewalls, encryption);
- (e) processes designed to prevent, detect, and eradicate malicious software;
- (f) procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

## **2. Access Control**

**2.1 Identification and Authentication.** Access to Juvenile Case File Information or any Research Entity Processing Resources shall be Identified and Authenticated as defined in this Section. "Identification" refers to processes that establish the identity of the Person requesting access to Juvenile Case File Information and/or Research Entity Processing Resources. "Authentication" refers to processes that validate the purported identity of the requestor. For access to Juvenile Case File Information or Research Entity Processing Resources, Research Entity shall require Authentication by the use of an individual, unique user ID and an individual password or other appropriate Authentication technique. Research Entity shall maintain procedures for the protection, integrity, and complexity of any passwords created by Research Entity and/or used by Research Entity in connection with the performance of Services. Passwords shall, at minimum, meet the complexity requirements defined by the United States Government Configuration Baseline (USGCB).

**2.2 Account Administration.** Research Entity shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Research Entity Processing Resources and Juvenile Case File Information, and shall include procedures for granting and revoking emergency access to Research Entity Processing Resources.

**2.3 Access Control.** Research Entity shall maintain appropriate access control mechanisms to prevent access to Juvenile Case File Information and/or Research Entity Processing Resources, except by authorized users. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Research Entity shall maintain processes to revoke access to Juvenile Case File Information within 48 hours after any Personnel of Research Entity are terminated, or immediately in the case of a non-voluntary termination. Research Entity shall maintain appropriate mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized attempts to access Juvenile Case File Information or Research Entity Processing Resources.

## **3. Personnel Security**

**3.1 Access to Juvenile Case File Information.** Research Entity shall require its personnel who have, or may be expected to have, access to Juvenile Case File Information to comply with the provisions of the Agreement, including this Addendum. Research Entity shall remain responsible for any breach of this Addendum by its personnel.

**3.2 Security Awareness.** Research Entity shall ensure that its employees and approved Research Entity remain aware of its security practices, and their responsibilities for protecting Juvenile Case File Information. This shall include:

- 3.2.1** protection against any form of malicious software;
- 3.2.2** appropriate password protection and password management practices;
- 3.2.3** appropriate use of workstations and computer system accounts; and



3.2.4 security and privacy training as appropriate.

**3.3 Sanction Policy.** Research Entity shall maintain a sanction policy to address violations of Research Entity's internal security requirements or security requirements that are imposed on Research Entity by law or contract.

#### **4. Risk Management**

**4.1 General Requirements.** Research Entity shall maintain appropriate safeguards and controls and exercise due diligence to protect Juvenile Case File Information and Research Entity Processing Resources against unauthorized access, use, and/or disclosure, considering:

4.1.1 applicable law;

4.1.2 information technology industry practices;

4.1.3 the sensitivity of the data; and

4.1.4 the relative level and severity of risk of impact should the integrity, confidentiality, or availability of the data be compromised, as determined by Research Entity as part of an overall risk management program.

**4.2 Security Evaluations.** Research Entity shall periodically evaluate its processes and systems to ensure continued compliance with obligations imposed by law or contract with respect to the confidentiality, integrity, availability, of Juvenile Case File Information and Research Entity Processing Resources. Research Entity shall document the results of these evaluations and any remediation activities taken in response to these evaluations.

**4.3 Internal Records.** Research Entity shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, Research Entity shall take appropriate action to address and remediate identified vulnerabilities to Juvenile Case File Information and Research Entity Processing Resources.

**4.4 Audits.** In addition to any audit rights in the Agreement, audits shall be permitted at the request of the County to evaluate compliance with this Addendum.

#### **5. Physical Security**

**5.1** Research Entity shall maintain appropriate physical security controls (including facility and environmental controls) designed to prevent unauthorized physical access, tampering and theft to Research Entity Processing Resources and areas in which Juvenile Case File Information is stored or processed. Research Entity shall adopt and implement a written facility security plan that documents these

controls and the policies and procedures through which these controls will be maintained. Research Entity shall maintain appropriate records of maintenance performed on Processing Resources and on the physical control mechanisms used to secure Processing Resources.

## 6. **Communications Security**

- a. **Exchange of Confidential Information.** The Parties shall utilize a secure method of transmission when exchanging Juvenile Case File Information electronically.
- b. **Encryption.** Research Entity shall maintain encryption, in accordance with standards mutually agreed upon between the Parties, for all transmission of Juvenile Case File Information via public networks (e.g., the Internet). These transmissions include:
  - i. sessions between web browsers and web servers;
  - ii. email containing Juvenile Case File Information (including passwords); and
  - iii. the transfer of files via the Internet (e.g., SFTP).
- c. **Protection of Storage Media.** Research Entity shall ensure that storage media containing Juvenile Case File Information is properly and adequately sanitized of all Juvenile Case File Information or is destroyed prior to disposal or re-use for non-Research Entity processing. All media on which Juvenile Case File Information is stored shall be protected against unauthorized access or modification. Research Entity shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for Research Entity processing or on which Juvenile Case File Information has been stored.
- d. **Data Integrity.** Research Entity shall maintain processes designed to prevent unauthorized or inappropriate modification or destruction of Juvenile Case File Information. Research Entity shall, at its expense, use commercially reasonable efforts to correct any data that has been corrupted by Research Entity, its authorized Research Entity or its or their personnel.

## 7. **Security Incident Monitoring and Response**

- 7.1 **Security Incident Response.** Research Entity shall maintain processes to detect, identify, report, respond to, and resolve Security Incidents in a timeframe consistent with guidance provided by US-CERT, which can be found here: <https://www.us-cert.gov/government-users/reporting-requirements>

## 8. **Indemnification**

8.1 In addition to the indemnification language in the Agreement, Research Entity agrees to be responsible for, and defend, indemnify and hold harmless the County for any Security Incident caused by Research Entity's failure to meet its security and other obligations under the Agreement and this Addendum.

## 9. Research Entity System Management Requirements

### 9.1 Vulnerability and Patch Management

- a. **All Research Entity Managed Systems.** For Research Entity Managed Systems, Research Entity shall install and maintain ICSA Labs certified Anti-virus Software and, to the extent possible, use real time protection features. Research Entity shall maintain the Anti-virus Software in accordance with the Anti-virus Software vendor's recommended practices. In addition, Research Entity shall ensure that: (i) the Anti-virus Software checks for new Anti-virus Signatures no less than once per day and (ii) the related Anti-virus Signatures are current and no less recent than two versions/releases behind the most current version/release of the Anti-virus Signatures for the Anti-virus Software
- b. For Research Entity Managed Systems, Research Entity shall provide for prompt application of security updates for operating systems used on the Research Entity platform

### 9.2 System Hardening

- 9.2.1 Research Entity shall ensure unnecessary services and ports are disabled prior to implementation. Review and apply recommendations from <https://nvd.nist.gov/>.

### 9.3 Authentication

- 9.3.1 Research Entity shall assign a unique user ID to any Agent or end user who accesses Confidential Information on Research Entity Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.
- 9.3.2 Unless otherwise agreed by County, Research Entity shall ensure that Research Entity Managed Systems will require Strong Password for user authentication.

### 9.4 Data Protection

- 9.4.1 Research Entity shall implement processes and/or controls to prevent the accidental disclosure of County Sensitive Data to other Research Entity customers.

### 9.5 Account termination

**9.5.1** Research Entity shall disable user accounts of Agents or County end users for the system within five (5) business days of becoming aware of the termination of such individual. In the cases of cause for termination, Research Entity will disable such user accounts as soon as administratively possible.

## **9.6 System/data access**

**9.6.1** Research Entity and its Agents shall only access system, application or data which they are expressly authorized by County to access, even if the technical controls in the system or application do not prevent Research Entity or its Agent from accessing those data or functions outside of County's authorization. Research Entity shall impose reasonable sanctions against any Agent who attempts to bypass security controls.

**9.6.2** Research Entity agrees to use the Principle of Least Privilege when granting access to Research Entity Managed Systems or Juvenile Case File Information.

## **9.7 System maintenance**

**9.7.1** Research Entity shall maintain system(s) that generate, store, transmit or process County Sensitive Data according to manufacturer recommendations. Research Entity shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.

## **10. Software / System Capability**

### **10.1. Supported Product.**

**10.1.1** Unless otherwise expressly agreed by County in writing, Research Entity shall provide County only supported versions of the Product, which will not become "end of life" for at least 24 months. When the Product or Service requires third party components, Research Entity must provide a Product that is compatible with currently supported third party components. Unless otherwise expressly agreed by County, Research Entity represents that all third-party components in its Product are currently supported, are not considered "end of life" by the third-party provider of such components, and will not become "end of life" in less than 24 months from the date of acquisition by County.

**10.1.2** If Open Source Software is incorporated into the Product, Research Entity shall only use widely supported and active Open Source Software in the Product and shall disclose such software to County prior to its acquisition of the Product.

### **10.2. Software Capabilities Requirements.**

**10.2.1** Research Entity's Product shall support a configurable Session Timeout for all users or administrative access to the Product.

10.2.2 Research Entity shall ensure that Products provided can be configured to require a Strong Password for user authentication.

10.2.3 Research Entity's Product shall allow user accounts to be disabled after a configurable amount of failed login attempts over a configurable amount of time.

**IV.**

**10.3 Backdoor Software.** Research Entity shall not provide Products with Backdoor Software, including, without limitation, undocumented or secret access functions (e.g., accounts, authorization levels, over-rides or any backdoor). Research Entity shall supply all information needed for the County to manage all access (local or remote) capabilities within the Product including denying of Remote Access entirely from any party including Research Entity. Research Entity shall not include any feature within the Product that would allow anyone to circumvent configured authorization remotely.

**10.4. Remote Access Software.** Research Entity shall not provide Products that will allow for Remote Access from untrusted networks by default.