FOR OFFICIAL USE ONLY

AUTOMATED REENTRY MANAGEMENT SYSTEM (ARMS) DATA SHARING AGREEMENT

Between

THE CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION

and

COUNTY OF SANTA CLARA, OFFICE OF THE COUNTY EXECUTIVE
for

COMMUNITY AND REENTRY SERVICES

ARMS DATA SHARING SECURITY AGREEMENT

Agreement is made at Sacramento California on March 20, 2018 by and between the California Department of Corrections (CDCR) and County of Santa Clara, Office of the County Executive (Provider) (Contract Number and Contract Term TBD) to deliver Provider access to and use of the Automated Reentry Management System (ARMS) developed by CDCR.

This ARMS Data Sharing Agreement (DSA) is an attachment to the agreement establishing the Parolee Reentry Services Program between CDCR and **PROVIDER** entered on March 18, 2014, for the period of March 18, 2014 through June 30, 2016 (Agreement Number #5600004258).

1.0 This ARMS DSA is entered into by and between the Administrators of the CDCR and Provider to establish the content, use, and protection of data described below (ARMS Data) needed by Provider to support the contracted service, whether such data is provided by CDCR or collected by Provider on behalf of CDCR.

2.0 The ARMS closes a significant gap in information for offenders treated with rehabilitation programming by contracted providers. While ARMS will accumulate significant data, the data will need to be shared with other stakeholders throughout the rehabilitation process to ensure the process of rehabilitation is effective. The concept of operations within ARMS includes security and protection for Personal Health Information (PHI) and Personally Identifiable Information (PII). The data in ARMS has been classified as Moderate according to Federal Information Processing Standard (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems and the ARMS solution has been contracted to provide Federal Risk and Authorization Management Program (FedRAMP) standards for technical implementation to protect information maintained in the "Cloud."

3.0 In order to ensure the security of the ARMS Data the Provider agrees to permit CDCR or its authorized representatives to make online inspections at any time, or onsite inspections during regular business hours, for the purpose of conducting program and/or performance audits to ensure Provider is preserving the security of CDCR electronic data. CDCR is authorized to investigate reports of Provider misuse of electronic data. During such security audit or investigation, Provider shall comply with CDCR requests in providing access to its employees, together with records, books and correspondence, hardware and/or electronic files, and other documentation or media of every kind directly related to this ARMS DSA that are necessary for CDCR to carry out such security audit and investigation.

4.0 ARMS Data includes each of the types of information listed below. For purposes of this ARMS DSA the following definitions apply:

a. Public Information (PI) – information maintained by CDCR that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws (SAM §5320.5).

b. Confidential Information (CI) – information maintained by CDCR that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws (SAM §5320.5).
c. High Risk Confidential Information (HRCI) - Non-public information that if disclosed could result in a significant harm (including financial, legal, risk to life and safety or reputational damage) to the CDCR or individual(s) if compromised through alternation, corruption, loss, misuse, or unauthorized disclosure. Examples of HRCI include, but are not limited to, information such as the following:
    i. Personally identifiable information such as a person's name in conjunction with a person's social security, credit or debit card information, individual financial account, driver's license number, state ID number, or passport number, or a name in conjunction with biometric information;
    ii. Personal health information such as any information about health status, provisions of health care, or payment for health care information as protected under the Health Insurance Portability and Accountability Act (HIPAA) of 1996;
    iii. Correctional Offender Record Information as defined in California PC §§ 13100-13104;
    iv. All IT infrastructure information that would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency, including but not limited to firewall and router configurations, server names, IP addresses, and other system configurations;
    v. Any Document which contains information identifying any Confidential Informant, or information provided, as defined in CCR Title 15, Section 3321;
    vi. Any documentation of information which contains information or data within any Gang Data Base as defined in Department Operations Manual (DOM) Section(s) 52070.22 through 52070.24;
    vii. Records of investigations, intelligence information, or security procedures as specified in the PRA Section 6254(f).
d. Sensitive Information (SI) – information maintained by CDCR that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of financial transactions and regulatory actions.
e. Protected Health Information (PHI) - is defined as any information, in any form, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that can be used to identify an individual.
    i. Alcohol and Drug Abuse Patient Records as defined in Code of Federal Regulations (CFR) Title 42, Part 2.

f. Personally Identifiable Information (PII) - any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

g. Family Education Rights and Privacy Act (FERPA) - schools must have written permission from the parent or eligible student in order to release any information from a student's education record except where authorized under 34 CFR § 99.31.

h. Criminal Offender Record Information (CORI) - means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders; and maintaining for each offender a summary of arrests, pretrial proceedings, nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release. Such information shall be restricted to that which is recorded as the result of an arrest, detention, or other initiation of criminal proceedings or of any consequent proceedings related thereto. It shall be understood to include, where appropriate, such items for each person arrested as the following:

   i. Personal identification.
   ii. The fact, date, and arrest charge; whether the individual was subsequently released and, if so, by what authority and upon what terms.
   iii. The fact, date, and results of any pretrial proceedings.
   iv. The fact, date, and results of any trial or proceeding, including any sentence or penalty.
   v. The fact, date, and results of any direct or collateral review of that trial or proceeding; the period and place of any confinement, including admission, release; and, where appropriate, readmission and rerelease dates.
   vi. The fact, date, and results of any release proceedings.
   vii. The fact, date, and authority of any act of pardon or clemency.
   viii. The fact and date of any formal termination to the criminal justice process as to that charge or conviction.
      a) The fact, date, and results of any proceeding revoking probation or parole.

   CORI shall not include intelligence, analytical, and investigative reports and files, nor statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

i. Authorized Persons – means (i) Authorized Employees; and (ii) Provider's contractors, agents, outsourcers, and auditors as disclosed as part of the initial contract Agreement with CDCR who have a need to know or otherwise access HRCI PII, PHI, FERPA, or CORI to enable Provider to perform its obligations under this Agreement, and who are bound in writing by confidentiality obligations sufficient to protect HRCI, PII, PHI, FERPA, or CORI in accordance with the terms and conditions of this ARMS DSA.

j. Security Breach – means (i) any act or omission that materially compromises either the security, confidentiality or integrity of ARMS Data or the physical, technical,

administrative or organizational safeguards put in place by Provider (or any Authorized Persons) that relate to the protection of the security, confidentiality or integrity of personal information, or (ii) receipt of a complaint in relation to the privacy practices of Provider (or any Authorized Persons) or a breach or alleged breach of this Agreement relating to such privacy practices.

5.0. Period of Agreement

The period of this ARMS DSA shall be in effect for the time Provider is on contract, July 1, 2018 through June 30, 2021, to provide rehabilitation services with CDCR and making use of the CDCR ARMS Software as a Service (SaaS) solution, unless earlier terminated by 30-day written notice by either organization. The ARMS DSA is to be reviewed not less than every three years from the date of this ARMS DSA coordinated by the CDCR Information Security Officer (ISO). In the absence of this ARMS DSA, Provider may be prevented from retaining a contract for services.

6.0. Intended Use of ARMS Data

By this Agreement CDCR has appointed Provider as a licensed user organization of ARMS and ARMS Data. ARMS Data will be uploaded into ARMS from various CDCR systems for the purpose of ensuring contracted providers in ARMS have data necessary to make continuity of care decisions. Provider is granted permission for the use of the ARMS Data and is a caretaker or custodian of the ARMS data.

7.0. Constraints on Use of ARMS Data

All ARMS data to which CDCR provides access to Provider or which is collected by Provider on behalf of CDCR's employees is the property of CDCR, and shall not be sold, loaned, licensed, given, assigned, or in any way shared with third parties without the express prior written permission of the CDCR ISO. Data will be entered by Provider to the ARMS as well as by CDCR staff members from multiple divisions into the hosted application. The CDCR ARMS data shall not be sold or used, internally or externally, for any purpose not directly related to the scope of work defined in this agreement without the express prior written permission of the CDCR ISO. This duty extends to all authorized persons, agents, and employees of the Provider. This obligation survives the termination of this Agreement.

8.0. ARMS Data Security

Provider shall employ industry best practices, both technically and procedurally, to protect all ARMS Data from unauthorized physical and electronic access. Methods employed are subject to review and approval by CDCR at such times and with such frequency as CDCR deems necessary.

a. ARMS Data Elements

ARMS Data shared with Provider shall be limited to the data elements specifically defined and authorized by CDCR for use by Provider. Data collected within ARMS includes data to meet application requirements. If Provider wishes to collect additional data within ARMS other than that directed through CDCR requirements, Provider must submit a request in writing to CDCR. Under no circumstances shall Provider collect any information classified as SI or CI without the express prior written approval of the CDCR ISO. Data to be shared or collected shall be strictly limited to the elements defined within the ARMS specifications, including interfacing or uploaded data files for use in ARMS.

b. ARMS Data Handling Requirements

ARMS Data handling requirements may vary depending on the classification of ARMS Data shared with Provider. However, it is anticipated that most ARMS Data shared with Provider will involve a mix of classes of ARMS Data including SI,CI, HRCI, PHI, PII, or CORI. Therefore, whenever ARMS Data elements are aggregated for collection, transmission, or storage, the aggregate ARMS Data shall be handled using the protocols that apply to the most sensitive ARMS Data element.

c. In the general course of business with CDCR rehabilitative programming, the Provider must handle and treat ARMS Data of all types in full compliance with the following provisions as a general standard of care:
    i. Provider acknowledges and agrees that in the course of its engagement may receive or have access to some or all of the types of confidential ARMS Data listed above. Provider shall comply with the terms and conditions set forth in this Agreement in its collection, receipt, transmission, storage, disposal, use and disclosure of such ARMS Data and be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of ARMS Data under its control or in its possession by all Authorized Persons. Provider shall be responsible for, and remain liable to, CDCR for the actions and omissions of all Authorized Persons that are not Authorized Employees concerning the handling or treatment of ARMS Data as if they were Provider's own actions and omissions.
    ii. ARMS Data is deemed to be Confidential Information of CDCR and is not Confidential Information of Provider. In the event of a conflict or inconsistency between this Section and the ARMS DSA to which this ARMS DSA is added by this Attachment or Amendment, the terms and conditions set forth in this Section shall govern and control.
    iii. In recognition of the foregoing, Provider agrees and covenants that it shall:
        a) Keep and maintain all ARMS Data in strict confidence to avoid unauthorized access, use, or disclosure.

b) Use and disclose ARMS Data solely and exclusively for the purposes for which the data, or access to it, is provided pursuant to the terms and conditions of this ARMS DSA, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available ARMS Data for Provider's own purposes or for the benefit of anyone other than CDCR, in each case, without CDCR ISO prior written consent. Release of information including any data from ARMS to the media in any fashion that identifies client or CDCR individuals is prohibited. Aggregate summarization of data for programs may be shared if no individual information is disclosed. Examples include: types of programs offered, number of individuals in programs, length of programs, completion rate averages, etc.

c) Not, directly or indirectly, disclose ARMS Data to any person other than its Authorized Persons, including any, subcontractors, agents, lessees, licensees, outsourcers, or auditors (an "Unauthorized Third Party"), without the express prior written consent from the CDCR ISO unless and to the extent required by Government Authorities or as otherwise, to the extent expressly required, by applicable law, in which case, Provider shall (i) notify CDCR before such disclosure or as soon as possible but not later than 48 hours; (ii) be responsible for and remain liable to CDCR for the actions and/or omissions of such Unauthorized Third Parties concerning the treatment of such ARMS Data as if they were the Provider's own actions and/or omissions; and (iii) require the Unauthorized Third Party that has access to ARMS Data to execute a written agreement agreeing to comply with the terms and conditions of this Agreement relating to the treatment of ARMS Data.

iv. Provider User Management

a) Provider agrees to submit each ARMS user for CDCR program review and approval in accordance with program contract terms and conditions. CDCR reserves the right to require Provider to remove any user which CDCR determines is unqualified to continue to have access to ARMS.

b) In the event that the employment of a Provider employee or sub-contract entity or person who utilizes an ARMS user account for the CDCR program, is terminated for cause, or whose employment is terminated or ended for any reason, Provider agrees that the Providers local Site Administrator will inactivate the ARMS user's account immediately.

c) Provider agrees to inform CDCR of any change in the status of an ARMS user, including those referenced this section within one (1) business day.

d) CDCR reserves the right to inspect Provider user status change records in accordance with Section 3 of this ARMS DSA.

v. Provider shall exercise care for ARMS Data that is brought into ARMS, but not entered by Provider. ARM S Data not entered by Provider will be released to Provider for one offender at a time if the following conditions are met to facilitate Provider's control and responsibility (Provider may be required to perform these functions to facilitate their own continuity of care for clients managed in ARMS):
   a) The offender has signed a release of information (ROI) and that ROI is loaded into ARMS and verified prior to granting access to data other than that input by the program.
   b) The Provider is under contract with CDCR as a provider or as a subcontractor to Provider.
   c) Referral information may go to any provider and will not include information that is not releasable to the public.
   d) Providers can only view information on offenders that are referred to them for rehabilitation services and upon acceptance of that referral with the intent to enroll the offender.

vi. Providers must ensure that their staff members are authorized to perform in appropriate roles for the information they will be handling. This will include roles that have access to medical information that must have the need to know and require the data for performing their function. The Health Information Portability and Accountability Act (HIPAA) governs the use of medical data; however, mental health information is further controlled to DAPO clinicians (internal or contracted) for mental health specified programs within ARMS. The CFR 42, Part 2 governs the use of alcohol and drug abuse patient records. Education data for clients shall be managed in compliance with the Family Educational Rights and Privacy Act (FERPA).

vii. Providers are permitted to use the data provided to them online in ARMS for the purposes of delivering contracted services to referred clients only. Providers are also permitted to upload data to ARMS; however, whatever data is uploaded to ARMS must be treated as ARMS data for the purpose of any further sharing from ARMS.

viii. When typing, keying, or in any way entering data into ARMS in open text fields, there are mandatory restrictions to the data entered in these fields. Images and documents uploaded to ARMS also cannot have the data in this section included. Under no circumstances should the following data be entered into text fields or included in uploaded images or documents (this information must be part of annual training):
   a) Any specific (named) gang affiliations.
   b) Any information that could identify any victims of the clients.
   c) Any information that could identify witnesses of events related to the clients.
   d) Specific offenses for which clients were convicted.
   e) Offender enemy information.

f) The CDCR program area data unit will audit text fields for inappropriate information pertinent to this clause.

ix. If providers elect to download data from ARMS for uploading to their systems, the following provisions must be in effect at all times:
   a) The data must be protected (encrypted) at all times in storage or in transit.
   b) The data may be uploaded to provider systems to allow their systems to support their business model, invoicing, and other appropriate purposes. Data is still the property of the State and must be protected in provider systems from further inspection or use under the same conditions as if it were in ARMS (HIPAA, FERPA, etc.).
   c) CDCR data must not be further exchanged with any other system or entity electronically or manually unless specifically authorized in writing by the CDCR ISO.
   d) CDCR reports of data must not be shared for other than business purposes in support of State funded program services each provider is under contract to provide.
   e) Data download files or extracts from ARMS must be destroyed promptly once the data is uploaded to other systems.

x. Training will be made available by the CDCR program area data unit on conditions requiring release of information and data handling or sharing for any reason related to ARMS data. Providers must ensure each employee is trained in these conditions prior to using ARMS and on an annual basis and certify this training is complete within ARMS on an annual basis. Training will include:
   a) Roles that are required by contracts to handle and protect specific types of data.
   b) Conditions under which data can be seen by users.
   c) Conditions under which data from ARMS can be extracted for external use and how that data must be handled and protected if extracted.
   d) User responsibility to protect data in Provider environment.
   e) Requirement to destroy all data extracts when no longer under contract with CDCR. Destruction includes elimination of the possibility to recreate the file from any non-application source. Paper files and data in protected systems can be maintained for contract required durations.
   f) Methods to clear all CDCR data from enterprise systems in the event of a mandatory closure or if the Provider goes out of business.
   g) Methods to ensure that no data shall be shared beyond Provider's own systems needed for activity invoicing. No exceptions are allowed.

h) Training to ensure that the Provider takes appropriate measures to ensure that all its agents, partners and subcontractors comply with all the provisions herein. PRA requests shall be referred to the CDCR contract point of contact and Title 15 for information that can be released to the public.
i) Training as to what information is prohibited for open text fields.

9.0. Network Security

a. Internet Access to ARMS

Connections to Provider computers utilizing the Internet, whether for client access or remote administration, must be protected at all times using any of the following industry standard cryptographic technologies: SSL/TLS, IPSec, SSH/SCP, PGP.

b. Data Storage

Regardless of the media employed (i.e., disk, tape, etc.), data must be stored at all times in an encrypted format. Encryption algorithms shall be AES-128 or better, or Triple-DES (3-DES). The use of other encryption algorithms for data storage must be approved in writing by CDCR ISO. Approval may be granted or withheld at CDCR's sole discretion. CDCR ISO reserves the right to inspect all storage systems during business hours to ensure the continued security of the ARMS Data.

10.0. Compliance with Applicable Laws and Regulations

Provider shall at all times comply with all applicable federal laws and regulations protecting the privacy of citizens including CFR 42, Part 2; the FERPA; and the HIPAA. Where applicable, Provider shall also comply with all provisions of the Financial Services Modernization Act (the "Gramm-Leach-Bliley Act").

11.0. Notification of Security Breaches

Provider agrees that in the event of any actual or suspected breach or compromise of the security, confidentiality or integrity of computerized data where ARMS Data of a CDCR employee, inmate, parolee, or ward was or is suspected to have been, acquired and/or accessed by an unauthorized person, Provider shall notify CDCR of the actual or suspected breach of the security system containing such data as soon as possible or at a minimum within 24 hours, comply with all notification actions, and/or assist CDCR with all notification actions required by State policy and the law.

CDCR contact for such notification is:

Vitaliy Panych
Agency Information Security Officer
Enterprise Information Services
California Department of Corrections and Rehabilitation
(916) 358-1959
Vitaliy.Panych@cdcr.ca.gov

Provider contact for such notification is:

Garry Herceg
Deputy County Executive
County of Santa Clara, Office of the County Executive
70 West Hedding Street, 11th Floor
San Jose, CA 95110
Phone: (408) 299-5125

12.0. Indemnification

Provider shall defend, indemnify, release, and hold CDCR harmless from and against all claims, demands, costs, damages, losses, and expenses arising out of or incidental to this ARMS DSA regardless of the negligence or fault of CDCR or any other entity or person, except in the event such loss due to the sole negligence or willful misconduct of CDCR.

13.0. Amendments, Attachments, Alterations, and Subcontracts Regarding This ARMS DSA

CDCR and Provider may only amend this ARMS DSA by mutual written consent.

a. Subcontract Flow Down Agreement

   All subcontracts entered into by Provider to delegate the performance of portions of this Agreement shall contain a provision by which the subcontractor to the Provider agrees to be bound to the Provider to perform its work in the same manner and under the same conditions as the Provider is bound to CDCR under this agreement.

14.0. Termination for Convenience or Cause

CDCR reserves the right to terminate this agreement for its convenience upon 30 days written notice. CDCR may terminate this Agreement for cause for the failure of Provider to cure a breach within the time stated in a notice thereof. Such termination may be without further notice. In the event CDCR terminates this Agreement, or Provider ceases operation,

Provider shall return to CDCR ISO all ARMS Data collected in the course of providing the application service. Provider shall certify in writing within five business days that all copies of the ARMS Data stored on Provider servers, backup servers, backup media, or other media have been permanently erased or destroyed. Destruction includes elimination of the possibility to recreate the file from any non-application source. Paper files of business services to CDCR clients and data in protected systems can only be maintained for contract required durations.

a. "Permanently erased" means the ARMS Data have been completely overwritten and are unrecoverable. File deletions or media high level formatting operations do not constitute a permanent erasure.

15.0. Suspension for Convenience

CDCR reserves the right to suspend the performance of this Agreement at the Department's sole discretion for such times and durations as CDCR deems necessary, upon five (5) days written notice to Provider.

16.0. Signatory Authority

By the signatures of their duly authorized representative below, CDCR and Provider, intending to be legally bound, agree to all of the provisions of this Data Sharing Agreement.

ARMS DATA SHARING SECURITY AGREEMENT

CDCR

RYAN SOUZA
Deputy Director
Program Support
Division of Rehabilitative Programs

Date

VITALIY PANYCH
Agency Information Security Officer
Enterprise Information Services

Date

NOTE: In the event a Provider has signed the DSA, but before CDCR has signed, and there has been a change in CDCR officers, CDCR shall attach an updated signature page so the current officers can sign.

CONTRACTED PROVIDER: COUNTY OF SANTA CLARA, OFFICE OF THE COUNTY EXECUTIVE.

Name Title Date

Approved as to Form and Legality

Deputy County Counsel

Date 3/13/15