

South Dakota Medical Cannabis Confidentiality and METRC API Agreement

1. PARTIES

a. This Confidentiality ("Agreement") is made as of this ____ day of _____ 2022 ("Effective Date") by and between _____ ("Provider") and the South Dakota Department of Health and Medical Cannabis Program ("State") (collectively the "Parties"), with respect to provision of one or more secondary software systems ("System," as further defined below) to one or more entities certified by the State to operate medical cannabis establishments in the State of South Dakota ("Licensees"). The Provider and the State hereby agree to the following terms and conditions.

b. **RENEWAL**

This agreement will not automatically renew. Provider must sign a new agreement each year and may be submitted via facsimile or e-mail to the State. Agreements are due before or on January 31st of the corresponding even year.

2. EFFECTIVE DATE AND NOTICE OF NONLIABILITY

The Agreement shall not be effective or enforceable until it is approved and signed by all Parties. The State shall not be liable for the performance of any of its obligations hereunder, or be bound by any provision hereof, prior to the Effective Date.

By entering into this Agreement, the State is under no obligation to appropriate funds for, or to make, any payments to Provider or any Licensee for any reason, including but not limited to the purpose of reimbursing Provider or Licensee for any payments or expenses Provider or any Licensee may make or incur, including, without limitation, any such payments or expenses made or incurred pursuant to any agreement between Provider and any Licensee. Nor shall any provision in this Agreement be construed as imposing liability on the State for any expenses Provider or Licensee may make or incur in connection with this Agreement or the performance of this Agreement. Provider expressly waives any claims asserting liability against State in connection with this Agreement or the performance of this Agreement.

3. RECITALS

a. **Consideration**

The Parties acknowledge that the mutual promises and covenants contained herein and other good and valuable consideration are sufficient and adequate to support this Agreement.

b. **Purpose**

Licensees are required to use the inventory tracking system developed by the State, currently known as METRC, as the primary inventory tracking system of

record. Licensees are also permitted to use a 3rd party system in conjunction with METRC. Licensees have requested the ability to establish an interface between such System and METRC. In order to communicate information electronically between METRC and the System this agreement is required. Licensee and patient information are subject to strict confidentiality. The State has agreed to permit Licensees to communicate information electronically to and from METRC through Provider's System or Services via an Application Programming Interface ("API"), but this permission is valid only if the Provider of the System enters an agreement to protect the confidentiality of the information/data contained in METRC and the State's Patient registration system. The Provider herein agrees to maintain data integrity and to comply with the security requirements set forth in this agreement.

4. DEFINITIONS

- a. "API" means the Application Programming Interface designed, developed, and maintained by the Seed to Sale System vendor assigned by the State, METRC.
- b. "API Key" means an alphanumeric code generated through METRC to gain programmatic access to METRC and automatic electronic communication of data and information between Provider's System and METRC. There are two Kinds of API Keys:
 - A. "Vendor API Key" means an API key that is specific to Provider and Provider's System, which must be used by every instance of Provider's System at all times, in combination with the User API Key specific to Licensee(s), in order to gain authorized programmatic access to METRC and automatic communication of data and information between Provider's System and METRC pertaining to such Licensee(s).
 - B. "User API Key" means an API Key that is specific to a particular Licensee, which only such Licensee is able and authorized to generate and obtain or deactivate. The User API Key may be deactivated by generating a new User API Key. The User API Key is linked directly to that Licensee's METRC account and allows access to that Licensee's METRC data and information.
- c. "Incident" means an accidental or deliberate event that results in or poses a threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State. Incidents include, but are not limited to: (i) successful attempts to gain unauthorized access to the METRC system or Confidential Information regardless of where such information is located; (ii) unwanted

disruption or denial of service attacks; (iii) the unauthorized use of METRC in any way; (iv) any unauthorized access by any person to Confidential Information, or (v) changes to the State's system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent.

- d. "Real Time" means relating to a system in which input data is processed within one second so that is available virtually immediately as feedback.
- e. "METRC" or "METRC system" means the cannabis inventory tracking system prescribed by the State to enable the State to track all legally grown cannabis from seed to sale, and also includes any successor inventory tracking system that the State permits or requires Licensees to utilize.
- f. "Payment Card Information (PCI) Data" means any data related to card holders' names, credit card numbers, or other credit card or financial information as may be protected by State and/or federal law.
- g. "Personally Identifiable Information (PII) Data" means information about an individual collected by the State or any other governmental entity that could reasonably be used to identify such individual and includes, but is not limited to, any combination of (i) first and last name, (ii) first name or first initial and last name, (iii) residence or other physical address, (iv) electronic mail address, (v) telephone number, (vi) birth date, (vii) PCI Data, (viii) social security number, (ix) driver's license number, (x) identification card number, or (xi) any other information that identifies an individual personally.
- h. "Provider Agreement" means an agreement between a Licensee and Provider entered into for the purpose of providing a System or Services to the Licensee.
- i. "Services" means the services to be performed by Provider to Licensee pursuant to the Provider Agreement in connection with the provision, operation or maintenance of the System.
- j. "Subcontractor" means any third party engaged by Provider to aid in performance of Provider's obligations to Licensee(s).
- k. "System" means the secondary software system provided by Provider for use by Licensee. Such Systems may be used to collect information to be used by the Licensees in operating their businesses, including, but not limited to, secondary inventory tracking and point of sale systems.
- l. "Provider" is a Licensee or 3rd Party Vendor working with a South Dakota Medical Cannabis Program Licensee.

5. CONFIDENTIAL INFORMATION

- a. “Confidential Information” means all information, data, records, and documentary materials which are of a sensitive nature regardless of physical form or characteristics, and includes, but is not limited to, non-public State records, sensitive State data, protected State data, PII Data, PCI Data, and other information. Data concerning individuals, patients and Licensees including financial information such as banking information, type(s) of medicine purchased and social security numbers, which has been communicated, furnished, or provided by the State’s seed to sale system (METRC) should be handled with care and proper due diligence.
- b. Any request or demand, including subpoenas, by a third party for Confidential Information in the possession or control of Provider shall be immediately forwarded to the State’s principal representative (Program Administrator of South Dakota Medical Cannabis Program) by the recipient of the request. The State shall have the right to move to quash any subpoena received from a third party seeking Confidential Information.
- c. Confidential information includes but is not limited to any information obtained by Provider through the interface between the METRC system and their System. Confidential Information may also include any information disclosed to Provider by Licensee, either directly or indirectly, in writing, orally, or through the communication of data through the API, whenever or however disclosed, including but not limited to: (i) names, addresses, or records of consumers’ personal information; (ii) consumer information or data; (iii) PII Data; (iv) PCI Data; (v) any other information that should reasonably be recognized as related to the PII Data of consumers; (vi) inventory tracking data, reports, or records related to the cultivation, manufacture, distribution, or sale of medical or retail marijuana or marijuana product, if such data, reports, or records are intended to be provided to the State through the METRC or otherwise; (vii) business plans and performance related to the past, present or future activities of such party, its affiliates, subsidiaries and affiliated companies; (viii) all types of Patient and Licensee data, including but not limited to, names and lists of other license holders, service providers, or affiliates; (ix) business policies, practices, and procedures; (x) names of employees; (xi) and any other information that should reasonably be recognized as related to business conducted by Licensee.

6. AUTHORIZATION

- a. The State hereby authorizes METRC to provide a Vendor API Key to Provider that must be used in combination with a Licensee’s User API Key to furnish Provider access regarding Licensee’s Patient information in the METRC system. This API key is used for the purposes of communicating real-time sales information to the METRC system. The authorization is granted for use by Licensee(s) in operating the business of such Licensee(s). This Agreement, and Provider’s rights and obligations hereunder, shall not be assigned without the prior written consent of the State, which may be approved or denied in the State’s sole discretion. Authorization by this contract grants Licensee the ability to Revoke a Vendor’s API Key and requires a Reconciliation process and accountability. Provider agrees to accept and abide by the current Metrc Web API

Documentation Best Practices which can be found
at <https://api-md.metroc.com/documentation#getting-started>

b. REVOKING A PROVIDER'S API KEY

A Licensee shall have the right to block a Provider's access to its data in METRC by deactivating such Licensee's User API Key and generating a new one or having METRC generate a new User API Key through METRC.

c. RECONCILIATION & ACCOUNTABILITY

A Licensee shall take full responsibility for ensuring all point of sale ("POS") transactions are accurately represented in the METRC system. Daily verification of reconciliation should occur to ensure proper reporting. Upon request, the Licensee shall provide the State with reporting verification that all POS transactions have been reconciled. The Provider of this agreement agrees to ensure their system can provide such reporting verification to Licensee.

d. Penalty: A verbal or written warning will be issued for the first (1st) offense of a Provider's system not reporting sale transactions of a Licensee and the Licensee may and shall have their User API key revoked, if future or recurring instances occur. Provider agrees that notwithstanding any contrary provision in a Provider Agreement, and in keeping with the State's obligation to maintain the confidentiality of Licensee(s) data and information, Provider expressly waives and shall not be entitled to seek or obtain injunctive, equitable or other relief against the State or METRC to compel the furnishing of any Licensee's User API Key to Provider. Licensee shall maintain, at all times, the right to terminate the Provider Agreement or otherwise discontinue use of Provider's System and Services. Nothing in this agreement supersedes the State's rights to act regarding violations of SDCL 34-20G and ARSD 44:90.

e. The Provider further agrees to operate in good faith and with fair judgement at all times when providing a System or Service that interfaces with the METRC system.

f. The State at its sole discretion, retains the right to revoke or withdraw a Vendor API key at any time for any reason set forth by the terms of use in this agreement.

g. Any business or company signing this Agreement is subject to the same rules and regulations defining the integrity and accuracy of data entered into the State's tracking system (METRC). Information entered into the system inaccurately or in violation of the State's rules or regulations could result in the States revocation of a Vendor's API key.

h. Misrepresentation or knowingly entering false information into the State's tracking system may result in the revocation of the vendor API key. Provider agrees to accept and abide by the current Metrc Web API Documentation Best Practices which can be found at <https://api-md.metroc.com/documentation#getting-started>

7. SECURITY REQUIREMENTS AND INCIDENT RESPONSE

- a. The Provider or Licensee agrees to abide by all applicable federal, State and local laws concerning information security and comply with current State and Department of Information Technology information security policy, located at <https://bit.sd.gov/docs/Information%20Technology%20Security%20Policy%20-%20Contractor.pdf>. Provider shall limit access to and possession of Confidential Data to only employees whose responsibilities reasonably require such access or possession and shall train such employees on the Confidentiality obligations set forth herein.
- b. The Provider agrees to notify the State when any Provider system that may access, process, or store State data or State systems is subject to unintended access or attack. Unintended access or attack includes compromise by a computer malware, malicious search engine, credential compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.
- c. The Provider further agrees to notify the State within twenty-four (24) hours, or earlier if possible, of the discovery of the unintended access or attack by providing notice via written or electronic correspondence to the Program Administrator, South Dakota Medical Cannabis Program.
- d. The Provider agrees to notify the State within twenty-four (24) hours if there is a threat to Provider's product as it pertains to the use, disclosure, and security of the State data.
- e. If an unauthorized use or disclosure of any Confidential Data occurs, the Provider must provide written notice to the State within one business day after Contractor's discovery of such use or disclosure and thereafter all information the State requests concerning such unauthorized use or disclosure.
- f. The Provider, within twenty-four (24) of discovery, shall report to the State any improper or non-authorized use or disclosure of Confidential Data. Provider's report shall identify:
 - (a) the nature of the unauthorized use or disclosure;
 - (b) the Confidential Data used or disclosed,
 - (c) who made the unauthorized use or received the unauthorized disclosure;
 - (d) what the Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and
 - (e) what corrective action the Provider has taken or shall take to prevent future similar unauthorized use or disclosure.
 - (f) The Provider shall provide such other information, including a written report, as reasonably requested by the State.

- g. The Provider shall protect Confidential Data according to a written security policy and shall

make available a copy of such policy to the state upon request. The Provider agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of Confidential Data or other event requiring notification. In the event of a breach of any of the Provider's security obligations or other event requiring notification under applicable law, the Provider agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the State and its officials and employees from and against any claims, damages, or other harm related to such security obligation breach or other event requiring the notification.

- h. The Provider shall disclose all of its non-proprietary security processes and technical limitations to the State.
- i. This Section shall survive expiration or termination of this Contract.

8. SECURITY INCIDENT OR DATA BREACH NOTIFICATION

- a. The Provider shall inform the State of any security incident or data breach.
- b. Incident Response: The Provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Agreement. Discussing security incidents with the State should be handled on an urgent basis, as part of Provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the Agreement.
- c. Security Incident Reporting Requirements: The Provider shall immediately report a security incident to the State's Program Administrator, Medical Cannabis Program, and mcquestions@state.sd.us.
- d. Breach Reporting Requirements: If the Provider has actual knowledge of a confirmed data breach that affects the security of any State content that is subject to applicable data breach notification law, the Provider shall (1) promptly notify the appropriate State-identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.
- e. **Data Breach Responsibilities**
 - A. This section only applies when a data breach occurs with respect to Confidential Data within the possession or control of the Provider.
 - B. The Provider, unless stipulated otherwise, shall immediately notify the appropriate State-identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
 - C. The Provider, unless stipulated otherwise, shall promptly notify the appropriate State-identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been, a data breach. The Provider shall (1) cooperate with the State to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and

- (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- D. Unless otherwise stipulated, if a data breach is a direct result of the Provider's breach of its Contract obligation to encrypt Confidential Data or otherwise prevent its release, the Provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State or federal law; (4) a website or a toll-free number and call center for affected individuals required by State law; and (5) complete all corrective actions as reasonably determined by Provider based on root cause; all [(1) through (5)] subject to this Contract's limitation of liability.

9. DATA PROTECTION

a. Data Ownership

The State will own all right, title and interest in its data that is related to the services provided by this contract. The Provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the State's written request.

b. Loss of Data

In the event of loss of any State data or records where such loss is due to the intentional act, omission, or negligence of the Provider or any of its subcontractors or agents, the Provider shall be responsible for recreating such lost data in the manner and on the schedule set by the Contract Manager. The Provider shall ensure that all data is backed up and is recoverable by the Licensee. In accordance with prevailing federal or state law or regulations, the Provider shall report the loss of non-public data as directed in this agreement.

- c. Protection of data and personal privacy (as further described and defined in this agreement) shall be an integral part of the business activities of the Provider to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Provider shall safeguard the confidentiality, integrity and availability of State information and comply with the following conditions:
- d. The Provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Confidential Data and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Provider applies to its own Confidential Data and non-public data of similar kind.
- e. All Confidential Data shall be encrypted at rest and in transit with controlled access, including back-ups. Unless otherwise stipulated, the Provider is responsible for the encryption of the Confidential Data. All data collected or created in the performance of this contract shall become and remain property of the State.
- f. Unless otherwise stipulated, the Provider shall encrypt all non-public data at rest and in transit. The State shall identify data it deems as non-public data to the Contractor. The level of protection and encryption for all non-public data shall be identified and made a part of this Contract.
- g. At no time shall any data or processes – that either belong to or are intended for the use of

the State or its officers, agents or employees – be copied, disclosed or retained by the Provider or any party related to the Provider for subsequent use in any transaction that does not include the State.

- h. The Provider shall not use any information collected in connection with the service issued under this Contract for any purpose other than fulfilling the service.

10. OTHER MANDATORY ITEMS

a. Data Location

The Provider shall provide its services to the State and its end users solely from data centers in the United States (“U.S.”). Storage of State data at rest shall be located solely in data centers in the U.S. The Provider shall not allow its personnel or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Provider shall permit its personnel and contractors to access State data remotely only as required to provide technical support. If requested by the State, the Provider shall provide technical user support on a 24/7 basis.

b. Import and Export of Data

The State shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Provider or Licensee. This includes the ability for the State to import or export data to/from third parties.

c. Encryption of Data at Rest

The Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Confidential Data, unless the State approves the storage of Confidential Data on a Provider portable device in order to accomplish Contract work.

11. REMEDIES

If Provider is in breach under any provision of this Agreement, the State shall have all of the remedies listed in this section in addition to all other remedies set forth in other sections of this Agreement. The State may exercise any or all of the remedies available to it, in its sole discretion, concurrently or consecutively.

a. Termination for Cause and/or Breach

The State may terminate this entire Agreement or any part of this Agreement. Exercise by the State of this right shall not be a breach of its obligations hereunder. Provider shall continue performance of this Agreement to the extent not terminated, if any.

A. Obligations and Rights

To the extent specified in any termination notice, Provider shall take timely, reasonable, and necessary action to protect and preserve Confidential Information in the possession or control of the Provider. All Confidential Information in the possession or control of Provider shall be immediately returned to the State as specified in this Agreement and Provider shall certify that no copies of Confidential Information remain in the possession or control

of Provider.

B. Vendor API Key Deactivation

Upon any breach of this Agreement, the State may deactivate Provider's Vendor API Key. Provider agrees that the Vendor API Key does not constitute any ownership and expressly waives any rights associated with the provision of information obtained with API Key. Provider specifically agrees it has no right to a hearing or other legal or administrative process regarding the deactivation of the Vendor API Key.

C. Damages

Notwithstanding any other remedial action by the State, Provider shall remain liable to the State for any damages sustained by the State by virtue of any breach under this Agreement by Provider.

D. Early Termination in the Public Interest

If this Agreement ceases to further the public policy of the State, the State, in its sole discretion, may deactivate Provider's Vendor API Key and terminate this Agreement. Exercise by the State of this right shall not constitute a breach of the State's obligations hereunder.

E. Remedies Not Involving Termination

The State, in its sole discretion, may exercise one or more of the following remedies in addition to other remedies available to it:

(a) Removal

Notwithstanding any other provision herein, the State may demand immediate removal of any of Provider's employees, agents, Subcontractors or permitted assigns whom the State deems incompetent, careless, insubordinate, unsuitable, or otherwise unacceptable, or whose continued relation to this Agreement is deemed to be contrary to the public interest or the State's best interest.

(b) Intellectual Property

If Provider infringes on a patent, copyright, trademark, trade secret, or other intellectual property right while performing the Services or providing the System, Provider shall, at the State's option (a) obtain the right to use such products and Services; (b) replace any goods, Services, or product involved with non-infringing goods, Services or products or modify such goods, Services or products so that they become non-infringing; or (c) if neither of the foregoing alternatives are reasonably available, remove any infringing goods, Services, or products.

12. OTHER PROVISIONS

- A. **CHOICE OF LAW AND FORUM.** The terms and conditions of this contract are subject to and will be construed under the laws of the State of South Dakota. The parties further agree that any dispute arising from the terms and conditions of this contract, which cannot be resolved by mutual agreement, will be tried in the Sixth Judicial Circuit Court, Hughes County, South Dakota.
- B. **INTEGRATION.** This contract is a complete version of the entire agreement between the parties with respect to the subject matter within this contract and supersedes all prior or contemporaneous written or oral understandings, agreements and communications between them with respect to such subject matter. This contract may be modified or amended only by a writing signed by both parties.
- C. **TERMINATION:** This contract may be terminated by either party hereto upon thirty (30) days written notice, and may be terminated by State for cause at any time, with or without notice.
- D. **NOTICE:** Any notice or other communication required under this contract shall be in writing and sent to the address set forth above. Notices shall be given by and to the State Contact Person on behalf of State, and by and to the Vendor Contact Person on behalf of Vendor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.
- E. **ASSURANCES:** The Vendor agrees to abide by all applicable provisions of the following assurances: Lobbying Activity, Byrd Anti Lobbying Amendment (31 USC 1352), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013, American Recovery and Reinvestment Act of 2009, and Section 106 (g) of the Trafficking Victims Protection Act of 2002, as amended (22 U.S.C. 7104) as applicable.
- F. **RESTRICTION OF BOYCOTT OF ISRAEL:** Pursuant Executive Order 2021-01, for contractors, vendors, supplies, or subcontracts with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars (\$100,000) or more, by signing this contract Vendor certifies and agrees that it has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to the subject matter of the contract, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for State to terminate this contract. Vendor further agrees to provide immediate written notice to State if during the term of the contract it no longer complies with this certification, and agrees such noncompliance may be grounds for contract termination.
- G. **CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:** Vendor agrees that neither Vendor, nor any of Vendor's principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions by any Federal department or agency. Vendor will provide immediate written notice to the Department of Health, Division of Administration (600 East Capitol Avenue, Pierre, SD 57501 (605) 773-3361), if Vendor, or any of Vendor's principals, becomes debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions involving Federal funding. Vendor further agrees that if this contract involves federal funds or federally mandated compliance, then Vendor is in compliance with all applicable regulations pursuant to Executive Order 12549, including Debarment and Suspension and Participants' Responsibilities, 29 C.F.R. § 98.510 (1990).
- H. **FUNDING TERMINATION:** This contract depends upon the continued availability of appropriated funds and expenditure authority from Congress, the Legislature or the Executive Branch for this purpose. This contract will be terminated for cause by State if Congress, the Legislature or Executive Branch fails to appropriate funds, terminates funding or does not grant expenditure authority. Funding termination is not a default by State nor does it give rise to a claim against State.
- I. **NONASSIGNMENT/SUBCONTRACTING:** Vendor shall not assign this contract, or any portion thereof, without the prior written consent of State. Vendor's assignment or attempted assignment of this contract, or any portion thereof, without State's prior written consent constitutes a material breach of contract. The Vendor may not use subcontractors to perform the services described herein without the express prior written consent of State. Vendor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage in a manner consistent with this Agreement. Vendor will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance.
- J. **FEDERAL AND STATE LAWS:** Vendor agrees that it will comply with all federal and state laws, rules and regulations as they may apply to the provision of services pursuant to this contract, including the Americans with Disabilities Act (ADA) of 1990, 42 U.S.C. §§ 12101-12213, and any amendment thereto, Section 306 of the Clean Air Act, and Section 508 of the Clean Water Act. Both parties further agree to provide services covered by this contract without regard to race, color, national origin, sex, age or disability as prohibited by state or federal law.
- K. **OWNERSHIP:** All reports, recommendations, documents, drawings, plans, specifications, technical data and information, copyrights, patents, licenses, or other products produced as a result of the services rendered under this contract, excluding medical records kept in the normal course of Vendor's business, will become the sole property of State. State hereby grants Vendor the unrestricted right to retain copies of and use these materials and the information contained therein in the normal course of Vendor's business for any lawful purpose. Either the originals, or reproducible copies satisfactory to State, of all

technical data, evaluations, reports and other work product of Vendor shall be delivered to State upon completion or termination of services under this contract.

- L. **REPORTING OF PERSONAL INJURIES AND/OR PROPERTY DAMAGE:** Vendor agrees to report promptly to State any event encountered in the course of performance of this contract which results in injury to the person or property of third parties, or which may otherwise subject Vendor or State to liability. Reporting to State under this section does not satisfy Vendor's obligation to report any event to law enforcement or other entities as required by law.
- M. **SEVERABILITY:** In the event that any term or provision of this contract shall violate any applicable law, such provision does not invalidate any other provision hereof.
- N. **AUDIT REQUIREMENTS:**
(EXPENDING \$750,000 OR MORE)
A nonprofit subrecipient, (as well as profit hospitals) (Vendor), expending \$750,000 or more in one year in Federal awards, must have an annual audit made in accordance with 2 CFR Chapter I, Chapter II, Part 200, et al. Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.
- All audits must be conducted by an auditor approved by the Auditor General to perform the audit. Approval may be obtained by forwarding a copy of the audit engagement letter to the Department of Legislative Audit, 427 South Chapelle, c/o 500 East Capitol, Pierre, SD 57501-5070. On continuing engagements, the Auditor General's approval should be obtained annually. The auditor must follow the Auditor General's guidelines when conducting the audit. The draft audit report must be submitted to the Auditor General for approval prior to issuing the final report. The auditor must file the requested copies of the final audit report with the Auditor General. Audits shall be completed and filed with granting agencies by the end of the ninth month following the end of the fiscal year being audited or 30 days after receipt of the auditor's report, whichever is earlier. If it appears that a required audit cannot be completed by the end of the ninth month following your fiscal year, you must request an extension from the federal agency for which the majority of federal expenditures relates.
- Failure to complete audit(s) as required will result in the disallowance of audit costs as direct or indirect charges to programs. Additionally, a percentage of awards may be withheld, overhead costs may be disallowed, and/or awards may be suspended, until the audit is completed satisfactorily.
- O. **FORCE MAJEURE:** Neither Vendor nor State shall be liable to the other for any delay in, or failure of performance of, any covenant or promise contained in this contract, nor shall any delay or failure constitute default or give rise to any liability for damages if, and only to the extent that, such delay or failure is caused by "force majeure". As used in this contract, "force majeure" means acts of God, acts of the public enemy, acts of the State and any governmental entity in its sovereign capacity, fires, floods, epidemics, quarantine restrictions, strikes or other labor disputes, freight embargoes, or unusually severe weather.
- P. **CONTRACT ORIGINAL AND COPIES:** An original of this contract will be retained by the State Auditor's Office. A photocopy will be on file with the South Dakota Department of Health and a second original will be sent to Vendor.
- Q. **RECORD RETENTION/EXAMINATION:** Vendor agrees to maintain all records that are pertinent to this contract and retain them for a period of three years following final payment against the contract. State agrees to assume responsibility for these items after that time period. These records shall be subject at all reasonable times for inspection, review or audit by State, other personnel duly authorized by State, and federal officials so authorized by law.
- R. **LICENSING AND COMPLIANCE:** The Vendor agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this agreement. The Vendor will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Vendor's failure to ensure the safety of all individuals served is assumed entirely by the Vendor.
- S. **CONFIDENTIALITY OF INFORMATION:** For the purpose of the sub-paragraph, "State Proprietary Information" shall include all information disclosed to the Vendor by the State. Vendor acknowledges that it shall have a duty to not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. Vendor shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this contract; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this contract; (iii) make State Proprietary Information available to any of its employees, officers, agents or Vendors except those who have agreed to obligations of confidentiality at least as strict as those set out in this contract and who have a need to know such information. Vendor is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. Vendor shall protect confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Vendor; (ii) was known to Vendor without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Vendor without the benefit or influence of the State's information; (v) becomes known to Vendor without restriction from a source not connected to the State of South Dakota. State's Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Vendor understands that this information is confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosure, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the contract except as required by applicable law or as necessary to carry out the terms of the contract or to enforce that party's rights under this contract. Vendor acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this contract for the State to take any action that the State reasonably

believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Vendor will be required to undergo investigation.

- T. CONFLICT OF INTEREST: Provider agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Provider expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.
- U. RECYCLING. State strongly encourages Vendor to establish a recycling program to help preserve our natural resources and reduce the need for additional landfill space.

The Parties have caused their duly authorized representatives to execute this Agreement as of the date set forth above.

Provider: _____

Print Name: _____

Title: _____

Email: _____

Phone #: _____

Signature: _____

Date: _____

South Dakota Medical Cannabis Program

Print Name: _____

Title: _____

Email: _____

Phone #: _____

Signature: _____

Date: _____