Seed to Sale Tracking System
Medical Marijuana Application Programming Interface User Agreement

Pursuant to 19 CSR 30-95.090, before beginning operations, all certified seed-to-sale tracking system entities shall sign this Agreement.

1. PARTIES

This Medical Marijuana Application Programming Interface (“API”) User Agreement ("Agreement") is made as of this ____ day of __________ 20____ ("Effective Date") by and between the certified seed-to-sale tracking system entity ____ (“Provider”) and the State of Missouri Department of Health and Senior Services Medical Marijuana Program (the “Department”), with respect to provision of one or more secondary software systems (the "System," as further defined below) to one or more entities licensed by the Department to operate medical marijuana facilities in the State of Missouri ("Licensees"). The Provider and the Department (collectively referred to as the “Parties”) hereby agree to the following terms and conditions.

2. EFFECTIVE DATE AND NOTICE OF NONLIABILITY

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

b. By entering into this Agreement, the Department 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, but not limited to, 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 Department 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 the Department in connection with this Agreement or the performance of this Agreement.

3. TERM

a. The parties intend for the provisions of this Agreement to remain in effect so long as the Provider remains certified to operate the System. This Agreement shall expire one year after its effective date unless renewed sooner, and the Parties shall renew this Agreement annually so long as the Provider remains certified, on or about the date that the Provider’s annual fee is due pursuant to 19 CSR 30-95.090(1)(C).

b. In the event of termination or expiration of this Agreement, Provider shall take timely, reasonable, and necessary action to protect and preserve Confidential Information (as defined below) in the possession or control of the Provider. All Confidential Information in the possession or control of Provider shall be immediately returned to the Department, and Provider shall certify that no copies of Confidential Information remain in the possession or control of Provider.

c. The provisions of Section 11, Security Requirements and Incident Response, shall survive the termination or expiration of this Agreement.

4. 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, including, but not limited to, the Department’s initial certification of the Provider.

5. PURPOSE

Licensees are required to use the inventory tracking method implemented by the Department, currently known as METRC, as the primary inventory tracking system of record. Licensees are permitted to use a certified provider’s secondary software system (“System”) in conjunction with METRC. Working with a certified provider, Licensees may establish an interface between the System and METRC. This Agreement is required in order for the Department and Provider to communicate information electronically between METRC and the System. Licensee and patient information are subject to strict confidentiality. The Department will permit Licensees to communicate information electronically to and from METRC through Provider's System via an API, but this permission is valid only if the Provider of the System enters into this Agreement to protect the confidentiality of the information/data contained in METRC and the Department’s patient registration system. The Provider agrees to maintain data integrity and to comply with the security requirements set forth in this agreement.

6. DEFINITIONS

a. “API” means the Application Programming Interface designed, developed, and maintained by 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 in every instance of access to 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. “Metrc LLC” means the company engaged by the Department to design, develop, provide, host and maintain the Department's METRC system, and also includes any successor organization.

d. “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 Department. 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 Department's system hardware, firmware, or software characteristics without the Department's knowledge, instruction, or consent.

e. “Real Time” means relating to a system in which input data is processed within one second so that is available virtually immediately as feedback.

f. “METRC” or “METRC system” means the medical marijuana inventory tracking system developed by Metrc LLC to enable the Department to track all legally grown marijuana from seed to sale, and also includes any successor inventory tracking system that the Department permits or requires Licensees to utilize.

g. “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 Department and/or federal law.

h. “Personally Identifiable Information (PII) Data” means information about an individual collected by the Department 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.

i. “Provider Agreement” means an agreement between a Licensee and Provider entered into for the purpose of providing a System or Services to the Licensee.

j. “Services” means the services to be performed by Provider for Licensee pursuant to the Provider Agreement in connection with the provision, operation, or maintenance of the System.

k. “Subcontractor” means any third party engaged by Provider to aid in performance of Provider's obligations to Licensee(s).

l. “System” means the secondary software system provided by Provider for use by a 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.

m. “Provider” is a seed-to-sale tracking entity certified by the Department to provide a System.

7. CONFIDENTIAL INFORMATION

a. "Confidential Information" means all information, data, records, and documentary materials that 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, personal identifying (PII) data, payment card industry (PCI) data, and other information or data concerning individuals and Licensees including financial information such as banking information and social security numbers, which has been communicated, furnished, or disclosed by the State to Provider. Confidential Information includes, but is not limited to, any information obtained by Provider through the interface between the METRC system and the 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 marijuana or marijuana product, if such data, reports, or records are or are intended to be provided to the State through the METRC system 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 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 a Licensee.

b. Any request or demand, including subpoenas and any public record requests submitted pursuant to RSMo Chapter 610 (the Missouri Sunshine Law), by a third party for Confidential Information in the possession or control of Provider, shall be immediately forwarded to the Department's Medical Marijuana Regulatory Program Director or his designee by the recipient of the request. The Department shall have the right to move to quash any subpoena or object to any public records request received from a third party seeking Confidential Information.

8. AUTHORIZATION

The Department hereby authorizes Metrc LLC 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 Department, which may be approved or denied in the Department'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.metrc.com/documentation#getting-started

9. 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 LLC generate a new User API Key through METRC.

10. RECONCILIATION & ACCOUNTABILITY

a. A Licensee shall be responsible for ensuring all point of sale 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 Department 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. The Department, either directly or through its agent or designee, may perform an audit of such reconciliations.

b. 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 Department'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 Department or Metrc LLC 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.

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

d. The Department, 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.

e. Any entity signing this Agreement is subject to any State of Missouri or Department rules and regulations defining the integrity and accuracy of data entered into METRC. Information entered into the system inaccurately or in violation of the State's or Department's rules or regulations could result in the Departments revocation of a Vendor's API key.

f. Misrepresentation or knowingly entering false information into the Department's tracking system may result in the revocation of the vendor API key.

g. API keys are non-transferable and cannot be shared. Sharing an API key with any entity outside of the legal entity, upon discovery, will result in the loss of the API key. Data entered into the API should be done on a transactional / real-time basis. The Vendor is required to perform a "GET" call on available dispensing limits before dispensing product to a patient or caregiver to prevent dispensing of product over that patient's certified limit. "Transactional" data is required to be entered into METRC via the UI, API, or any other means on a "real –time," or as close as possible to real-time, basis.

11. SECURITY REQUIREMENTS AND INCIDENT RESPONSE

a. The Provider agrees to abide by all applicable federal, State and local laws concerning information security and comply with current State of Missouri and Department information security policies, including but not limited to RSMo 407.1500. Provider shall limit access to and possession of Confidential Information to only those 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 Department when any Provider system that may access, process, or store Department data or Department 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 Department 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 Medical Marijuana Regulatory Program Director or his designee.

d. The Provider agrees to notify the Department within two (2) hours if there is a threat to Provider's product as it pertains to the use, disclosure, and security of the Department data.

e. If an unauthorized use or disclosure of any Confidential Information occurs, the Provider must provide written notice to the Department as soon as possible, but in no event more than one (1) business day, after Provider's discovery of such use or disclosure, and the notice shall identify:

   A. the nature of the unauthorized use or disclosure;
   B. the Confidential Information 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.

   The Provider shall provide such other information, including a written report, as reasonably requested by the Department.

f. The Provider shall protect Confidential Information according to a written security policy no less rigorous than that of the Department and shall supply a copy of such policy to the Department for validation. The Provider agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of Confidential Information 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 Department 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.

g. The Provider shall disclose all of its non-proprietary security processes and technical limitations to the Department.

h. This Section Eleven (11) shall survive expiration or termination of this Contract.

12. SECURITY INCIDENT OR DATA BREACH NOTIFICATION

a. In accordance with Section 11 above, the Provider shall immediately inform the Department of any security incident or data breach.

b. Incident Response: The parties acknowledge that the Department and the Provider may need to communicate with outside parties regarding any security incident, which may include contacting law enforcement, addressing media inquiries, and seeking external expertise. Provider shall treat all communications with the Department regarding such matters as urgent. The Provider shall discuss and coordinate any such response and communications with the Department.

c. Breach Reporting Requirements: If the Provider has actual knowledge of a confirmed data breach that affects the security of any Department content that is subject to any applicable data breach notification law, including but not limited to RSMo 407.1500 if applicable in the situation, the Provider shall (1) promptly notify the appropriate Department-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 and in accordance with applicable laws.

d. Unless otherwise stipulated, if a data breach is a direct result of the Provider's breach of its obligation to properly 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 the Department or by law; (3) a credit monitoring service required by Department or by law; (4) a website or a toll- free number and call center for affected individuals required by the Department or by law; and (5) completing all corrective actions as reasonably determined by Provider to address the root cause of the data breach.

13. DATA PROTECTION

a. Data Ownership- The Department will own all rights, title, and interest in its data that is related to this Agreement. 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 Department's written request.

b. Loss of Data- In the event of loss of any Department 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 Department. The Provider shall ensure that all data is backed up and is recoverable by the Licensee. In accordance with prevailing federal or Department 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 Department information at any time. To this end, the Provider shall safeguard the confidentiality, integrity, and availability of Department information as further indicated in this section.
d. The Provider shall implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Confidential Information 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 Information and non-public data of similar kind.
e. All Confidential Information 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 Information. All data collected or created in the performance of this contract shall become and remain property of the Department.
f. Unless otherwise stipulated, the Provider shall encrypt all non-public data at rest and in transit. The Department shall identify to the Provider the data it deems non-public. The level of protection and encryption for all non-public data shall be identified and made a part of this Agreement.
g. At no time shall any data or processes – that either belong to or are intended for the use of the Department 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 Department.
h. The Provider shall not use any information collected in connection with the service issued under this Agreement for any purpose other than fulfilling the service.

14. ADDITIONAL TERMS REGARDING DATA

a. Data Location -The Provider shall provide its services to the Department and its end users solely from data centers in the United States ("U.S."). Storage of

Department 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 Department 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 Department data remotely only as required to provide technical support. If requested by the Department, the Provider shall provide technical user support on a 24/7 basis.

b. Import and Export of Data- The Department shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Provider. This includes the ability for the Department 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 Department approves the storage of Confidential Data on a Provider portable device in order to accomplish System services.

d. Release of Data- The Provider shall contact the Department upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to the Department's data under this Agreement, or which in any way might reasonably require access to the data of the Department, unless prohibited by law from providing such notice. The Provider shall not respond to subpoenas, service of process and other legal requests related to the Department without first notifying the Department, unless prohibited by law from providing such notice.

e. Disposition of Data- The Department retains the right to use the System to access and retrieve Confidential Information stored on Provider's infrastructure at the State's sole discretion. Provider warrants, and shall cause each Subcontractor to warrant, that upon request of the State, the Department, or Provider, such Subcontractor shall submit its data processing facilities for an audit of its compliance with section 13 of this Agreement, including, but not limited to, the measures referred to in section 13. The State reserves its rights, title, and interest, including all intellectual property and proprietary rights, in and to METRC, METRC system data, Confidential Information, and all related data and content.

f. Safeguarding PII Data- If Provider will or may receive PII Data under this Agreement, Provider shall provide for the security of such PII Data, in a form acceptable to the State, including, but not limited to, nondisclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, and audits. Provider shall take full responsibility for the security of all PII Data in its possession, and shall hold the State harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof.

g. Safeguarding PCI Data- If Provider will or may receive PCI Data under this Agreement, Provider shall provide for the security of the PCI Data, in accordance with PCI Data Security Standard (DSS) 1.1. Security safeguards shall include, without limitation, supervision by responsible employees, approval of Subcontractors as required by State and/or federal law, non-disclosure of information other than as necessary in the performance of Provider's or Subcontractor's obligations under this Agreement, non-disclosure protections, proper accounting and storage of information, civil and criminal penalties for non-compliance as provided by law, certifications, and inspections.

15. REMEDIES

a. If Provider is in breach under any provision of this Agreement, the Department shall have all remedies available under the law including, but not limited to, those remedies expressly set forth in this Agreement. The Department may exercise any or all of the remedies available to it under the law, in its sole discretion, concurrently or consecutively.

b. Vendor API Key Deactivation- Upon any breach of this Agreement, the Department 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 Department, Provider shall remain liable to the Department for any damages sustained by the Department 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 Department, the Department, in its sole discretion, may deactivate Provider's Vendor API Key and terminate this Agreement. Exercise by the Department of this right shall not constitute a breach of the Department's obligations hereunder.

e. Remedies Not Involving Termination

The Department, in its sole discretion, may exercise the following remedies in addition to other remedies available to it:

A. Removal- Notwithstanding any other provision herein, the Department may demand immediate removal of any of Provider's employees, agents, Subcontractors, or permitted assigns whom the Department 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 Department'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 Department'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.

16. INDEMNIFICATION

a. Provider shall indemnify, defend, and hold the Department, its directors, officers, employees and agents harmless from liability for (a) tangible property damage, bodily injury and death, to the extent caused or contributed to by the Provider, (b) for the fraud or willful misconduct of the Provider, and (c) for the negligent, whether intentional or unintentional, misconduct of the Provider, and such indemnifications shall include all related defense costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties) arising from or relating to the performance of the Provider or its Subcontractors under this Agreement.

b. The Department has no obligation to provide legal counsel or defense to the Provider or its Subcontractors in the event that a suit, claim, or action of any character is brought by any person not party to this Agreement against the Provider or its subcontractors as a result of or relating to the Provider's obligations under this Agreement.

c. The Department has no obligation for the payment of any judgments or the settlement of any claims against the Provider or its Subcontractors as a result of or relating to the Provider's obligations under this Agreement. The Provider shall immediately notify the Department of any claim or suit made or filed against the Provider or its Subcontractors regarding any matter resulting from or relating to the Provider's obligations under the Agreement and will cooperate, assist, and consult with the Department in the defense or investigation of any claim, suit, or action made or filed by a third party against the Department as a result of or relating to the Provider's performance under this Agreement.

17. TERMINATION

The Department may terminate this entire Agreement or any part of this Agreement. Exercise by the Department 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, for the life of its certification and, section 11 shall survive any termination.

18. CHOICE OF LAW & NON ARBITRATION CLAUSE

This Agreement shall be construed, interpreted, and enforced according to the laws of the State of Missouri. Jurisdiction and venue over any litigation will occur in Cole County in the State of Missouri. No term or condition of this Agreement shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protections, or other provisions of law. The Parties agree that the Department retains any and all such immunities, rights, benefits, and protections. The Department does not agree to arbitration of any claims.

19. CONFLICT OF INTEREST

Provider has no interests and shall not acquire any interest, direct or indirect, that would conflict in any manner or degree with the performance of Provider's Services and Provider shall not employ any person having such known interests.

20. ENTIRE UNDERSTANDING

This Agreement represents the complete integration of all understandings between the parties and all prior representations and understandings, oral or written, are merged herein. Prior or contemporaneous additions, deletions, or other changes hereto shall not have any force or effect whatsoever, unless embodied herein. This Agreement may be executed in one or more counterparts, each counterpart to be considered an original portion of this Agreement, and all of which together shall constitute a single instrument. Facsimile and Portable Document Format ("PDF") copies of the Parties' signatures shall be treated as originals.

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

Signatures: