METRC SEED TO SALE SYSTEM USER AGREEMENT
DEPARTMENT OF HEALTH AND HUMAN RESOURCES,
BUREAU FOR PUBLIC HEALTH, OFFICE OF MEDICAL CANNABIS

f

This User Agreement ("Agreement") is made as of this _______day of_____, 2021 ("Effective Date") by and between____________("User"), ________________________, ("Permittee") and the West Virginia Office of Medical Cannabis ("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 permitted by the State to operate medical cannabis establishments in the State of West Virginia.

WHEREAS, entities permitted to grow, process, and/or dispense medical cannabis in West Virginia ("Permittees") are required by law to use the "Seed to Sale" inventory tracking system developed by the State, currently known as METRC, as the primary inventory tracking system of record (code citation). Permittees may use a third party system or provider in conjunction with METRC;

WHEREAS, the State requires execution of this Agreement to allow a data interface between the secondary software system of User and METRC for the communication of information electronically to and from METRC via an Application Programming Interface ("API"); and

WHEREFORE, based upon the foregoing, 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, and agree to the following terms and conditions:

A. DEFINITIONS

1. "API" means the Application Programming Interface designed, developed, and maintained by the Seed to Sale System vendor assigned by the State, METRC.
2. "API Key" means an alphanumeric code generated through METRC to gain programmatic access to METRC and automatic electronic communication of data and information between User's System and METRC. There are two Kinds of API Keys:
   a. "Vendor API Key" means an API key that is specific to User and User's System, which must be used by every instance of User's System at all times, in combination with the User API Key specific to Permittee(s), in order to gain authorized programmatic access to METRC and automatic communication of data and information between User's System and METRC pertaining to such Permittee(s).
   b. "User API Key" means an API Key that is specific to a particular Permittee, which only such Permittee 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 Permittee's METRC account and allows access to that Permittee's METRC data and information.

3. “Breach” means any use or disclosure of the Data in violation of the Agreement by the User, its governing body, employees, contractors or agents or by a third party to which the User disclosed the Data.

4. “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 and Permittees 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. Confidential information includes but is not limited to any information obtained by User through the interface between the METRC system and their System. Confidential Information may also include any information disclosed to User by Permittee, 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 Permittee data, including but not limited to, names and lists of other license holders, service Users, 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 Permittee.

5. “Data” means all Confidential Information and any other information stored in, or communicated to or from the METRC system.

6. “Franwell” means Franwell, Inc., the company engaged by the State to design, develop, provide, host and maintain the State's METRC system, and also includes any successor organization.

7. “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.

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

9. “METRC” or “METRC system” means the cannabis inventory tracking system developed by Franwell 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 Permittees to utilize.

10. “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.

11. “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.

12. “User Agreement” means an agreement between a Permittee and User entered into for the purpose of providing a System or Services to the Permittee.

13. “Services” means the services to be performed by User to Permittee pursuant to the User Agreement in connection with the provision, operation or maintenance of the System.

14. “Subcontractor” means any third party engaged by User to aid in performance of User's obligations to Permittee(s).

15. “System” means the secondary software system provided by User for use by Permittee. Such Systems may be used to collect information to be used by the Permittees in operating their businesses, including, but not limited to, secondary inventory tracking and point of sale systems.

B. AUTHORIZATION

The State agrees to authorize Franwell (METRC) to provide an API Key to User to be used in combination with the Permittee's User API Key allowing User access to information regarding Permittee’s Patient information in the METRC system. The API key is used for the purposes of communicating real-time sales information to the METRC system. The authorization is granted for use by Permittee(s) in operating the business of such Permittee(s). This Agreement, and User's rights and obligations hereunder, shall not be assigned without the prior written consent of the State and amendment to this Agreement, which may be approved or denied in the State's sole discretion. API key authorization by this Agreement allows Permittee and the State to Revoke a Vendor’s API Key. User agrees to accept and abide by the current Metrc Web API Documentation Best Practices which can be found at https://api-wv.metrc.com/documentation#getting-started.

C. REVOCATION OF API KEY

A Permittee or the State shall have the unilateral discretion to terminate a User's access to the Data in METRC by deactivating the User API Key or by requesting Franwell generate a new User API Key through METRC. Any action by the State to terminate User's access to METRC or otherwise deactivate User's access to METRC shall give rise to no cause of action or right of appeal by Permittee or User.

D. RECONCILIATION & ACCOUNTABILITY

1. A Permittee shall be responsible 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 Permittee shall provide the State with reporting verification that all POS transactions have been reconciled. The User of this agreement agrees to ensure their system can provide such reporting verification to Permittee.

2. User agrees that notwithstanding any contrary provision in any other agreement between any of the Parties, User expressly waives and shall not be entitled to seek or obtain injunctive, equitable or other relief against the State, Permittee or Franwell to compel the furnishing of any Permittee's User API Key to User.

3. The User further agrees to utilize the METRC system only in accordance with this Agreement.

4. 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. If State provides a warning to Use and/or Permittee or allows either User or Permittee the opportunity to cure, such action by the State shall not be a waiver of any of the State's rights or remedies under this Agreement.

5. Any party to 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 may result in the termination or revocation of a Vendor's API key.

6. Misrepresentation or knowingly entering false information into the State's tracking system may result in, among other things, the revocation of the vendor API key. User agrees to accept and abide by the current METRC Web API Documentation Best Practices which can be found at https://api-wv.metrc.com/documentation#getting-started

7. 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 shall be 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 the 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.

8. Any request or demand, including subpoenas, by a third party for Confidential Information or any other Data in the possession or control of User shall be immediately forwarded to the General Counsel of the West Virginia Department of Health and Human Resources and to the Executive Director of OMC 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.

E. DATA OWNERSHIP AND HANDLING

1. Data Ownership
   The State will own all right, title and interest in the Data. The User 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.

2. Data Location
   The User 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 User 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 User shall permit its personnel and contractors to access State data remotely only as required to provide technical support. If requested by the State, the User shall provide technical user support on a 24/7 basis.

3. 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 User or Licensee. This includes the ability for the State to import or export data to/from third parties.

4. Encryption of Data at Rest.
   The User 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 User portable device in order to accomplish Contract work.

5. Handling.
   The User shall handle Data only as permitted under the terms of this Agreement, and shall ensure that its governing body, employees, contractors and agents do not handle the Data in a manner that would constitute a violation of this Agreement.

6. Loss of Data
   In the event of loss of any Data where such loss is due to the activities of the User or any of its subcontractors or agents, the User shall be responsible for recreating such lost data in the manner and on the schedule set by the State. The User shall ensure that all data is

backed up and is recoverable by the Permittee. In accordance with prevailing federal or state law or regulations, the User shall report the loss of non-public data as directed in this Agreement.

7. 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 User to ensure there is no inappropriate or unauthorized use of Data at any time. To this end, the User shall safeguard the confidentiality, integrity and availability of Data and otherwise comply with the following conditions:

   a. The User 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 User applies to its own Confidential Data and non-public data of similar kind.

   b. All Confidential Data shall be encrypted at rest and in transit with controlled access, including back-ups. Unless otherwise stipulated, the User 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.

   c. 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 User or any party related to the User for subsequent use in any transaction that does not include the State.

   d. The User shall not use any information collected in connection with the service issued under this Agreement for any purpose other than fulfilling the service, and may disclose the Data only as permitted under the terms of this Agreement. The User will not in any manner, directly or indirectly, make known, disclose, publish or communicate the Data, or any part thereof, including but not limited to derivatives, to any person, firm, or corporation without the express written consent of the State.

   e. The User shall use appropriate and reasonable safeguards to prevent use or disclosure of the Data other than as permitted under this Agreement. The User shall make audit reports available upon the State’s request. The State or its designee may conduct audits of User’s security, including requesting a copy of the most current security policy.

   f. The User shall protect Data according to a written security policy no less rigorous than that of the State and shall supply a copy of such policy to the State for validation. The User agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of Data or other event requiring notification. In the event of a breach of any of the User's security obligations or other event requiring notification under applicable law, the User 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.

F. INCIDENT RESPONSE

1. The User and Permittee agree to abide by all applicable federal, State and local laws concerning information security and comply with current West Virginia State Privacy Office policies at: https://privacy.wv.gov/privacypolicies/Pages/default.aspx. User shall limit access to and possession of Data to only employees whose responsibilities reasonably require such access or possession and shall train such employees on the confidentiality obligations set forth herein.

2. The User agrees to immediately notify the State of an Incident, including any 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.

3. If the User has actual knowledge of unintended access or Breach, the User 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.

4. Upon the discovery of any Incident or Breach, if any Confidential Information or Data was, or is reasonably believed to have been, acquired by an unauthorized person, the vendor shall immediately notify: (1) The Director of OMC, (2) the DHHR privacy officer, Chris Snyder at: chris.s.snyder@wv.gov, and by calling 1-304-558-0684, and (3) the Office of Technology at incident@wv.gov. The User shall immediately investigate such actual or suspected Security Incident, Breach, or other unauthorized use or disclosure of Confidential Information or Data.

5. Within 24 hours of the discovery, if an actual Breach has occurred, the vendor shall notify the individuals identified in in the paragraph above of the following: (a) What data elements were involved and the extent of the data involved in the Breach (e.g. number of records or affected individual's data); (b) The identity of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI, Data or Confidential Information; (c) A description of where the Confidential Information or Data is believed to have been improperly transmitted, sent, or utilized; (d) A description of the probable causes of the improper use or disclosure; and (e) Whether any Federal or State laws requiring individual notifications of Breaches are triggered.

6. The State will coordinate with the User to determine additional specific actions that will be required of the vendor for mitigation of the Breach, which may include notification to the individual or other authorities, and may request a written report or other additional information from the User.

7. All associated costs shall be borne by the User. This may include, but not be limited to costs associated with notifying affected individuals.

8. These provisions are in addition to the provisions of the State of West Virginia Confidentiality Policies and Information Security Accountability Requirements found at: http://www.state.wv.us/admin/purchase/privacy/NoticeConfidentiality.pdf. The more stringent of that policy or the policies enumerated by this Agreement shall apply.

9. This Section shall survive expiration or termination of this Contract.

G. GENERAL TERMS

1. 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, or otherwise available at law for any violation of this Agreement. The State may exercise any or all of the remedies available to it, in its sole discretion, concurrently or consecutively.

2. API Key Deactivation. As stated above, the State may deactivate User's Vendor API Key. User agrees that the User API Key does not constitute any ownership and expressly waives any rights associated with the provision of information obtained with API Key. User specifically agrees it has no right to a hearing or other legal or administrative process regarding the deactivation of the User API Key.

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

4. Public Interest. If this Agreement ceases to further the public policy of the State, the State, in its sole discretion, may deactivate User's Vendor API Key and terminate this Agreement. Exercise by the State of this right shall not constitute a violation of any of State’s responsibilities, and the Data protections enumerated herein shall survive any such deactivation or termination.

5. Remedies Not Involving Termination or Revocation of API Key. The State, without waiving any of its rights hereunder, and in its sole discretion, may exercise one or more of the following intermediate remedies in addition to other remedies available to it:

   a. Notwithstanding any other provision herein, the State may demand immediate removal of any of User'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 User infringes on a patent, copyright, trademark, trade secret, or other intellectual property right while performing the Services or providing the System, User 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.

6. User shall indemnify, defend, and hold the State, its directors, officers, employees and agents harmless from liability for (a) tangible property damage, bodily injury and death, to the extent caused by or contributed to by the User, and (b) for the fraud or willful misconduct of the User, including 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 User or its Subcontractors under this Agreement.

7. The State has no obligation to provide legal counsel or defense to the User or its Subcontractors in the event that a suit, claim or action of any character is brought by any person against the User or its subcontractors as a result of or relating to the User's obligations under this Agreement.

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

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

10. This Contract shall be construed, interpreted, and enforced according to the laws of the State of West Virginia. Any litigation will be conducted in the state of West Virginia. The West Virginia Uniform Computer Information Transactions Act (Commercial Law Article, Title 22 of the Annotated Code of West Virginia) does not apply to this Agreement, the Software, or any Software license acquired hereunder.

11. 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. The Parties agree that the State retains all such immunities, rights, benefits, and protections.

12. The signatories of this agreement have no knowledge of a State employee having any

personal or beneficial interest whatsoever in the System or Services described in this Agreement. User has no interests and shall not acquire any interest, direct or indirect, that would conflict in any manner or degree with the performance of User's Services and User shall not employ any person having such known interests.

13. 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.

WHEREFORE, the Parties have caused their duly authorized representatives to execute this Agreement as of the date set forth below:

User: ____

Print Name: ____

Name: ____

Title: ____

Email: ____

Phone: ____

Signature: ____

Date: ____

User: ____

Print Name: ____

Name: ____

Title: ____

Email: ____

Phone: ____

Signature: ____

Date: ____

Permittee: ____

Print Name: ____

Title: ____

Email: ____

Phone: ____

Signature: ____

Date: ____

West Virginia Office of Medical Cannabis

Print Name: ____

Name: ____

Title: ____

Email: ____

Phone: ____

Signature: ____

Date: ____