Maryland Medical Cannabis Commission's
(MMCC)
Confidentiality & API USER AGREEMENT

1. PARTIES

a. This Confidentiality ("Agreement") is made as of this ____ day of _____ 2018 ("Effective Date") by and between _____ ("Provider") and the Maryland Medical Cannabis Commission ("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 licensed by the State to operate medical cannabis establishments in the State of Maryland ("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 even year (i.e. 2020, 2022, etc.) and may be submitted via facsimile or e-mail to MMCC. 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 MMCC'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. "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.

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 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.

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 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 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 State and/or federal law.

h. "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.

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 to 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 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.

A "Provider" is a Licensee or 3rd Party Vendor working with a MMCC 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 (Executive Director of MMCC) 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 Franwell (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.metrc.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 Franwell generate a new User API Key through METRC.

c. RECONCILIATION & ACCOUNTABILITY
A Licensee shall take full responsibility for ensuring all 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 Franwell 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.

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 / 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.metrc.com/documentation#getting-started

i. 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 their 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 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.

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 http://doit.maryland.gov/Publications/DoITSecurityPolicy.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 Contract Manager, MMCC’s Director of Information Technology.

d. The Provider agrees to notify the State within two (2) 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 (1) 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 one day 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 no less

rigorous than that of the State and shall supply a copy of such policy to the State 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 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 Contract. 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 Contract.

c. Security Incident Reporting Requirements: The Provider shall immediately report a security incident to the State's Contract Manager, MMCC's Director of Information Technology.

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 a 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. Indemnification
Provider 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 Provider, and (b) for the fraud or willful misconduct of the Provider, 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 Provider or its Subcontractors under this Agreement.

b. The State 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 State 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 State 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 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 Provider's performance under this Agreement.

d. The Provider 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 Provider 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.

13. MARYLAND LAW PREVAILS

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

14. Employee Financial Interest/Conflict of Interest.

a. 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. 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.

15. Entire Understanding

a. 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.

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: _____

Maryland Medical Cannabis Commission

Print Name: _____

Title: _____

Email: _____

Phone #: _____

Signature: _____

Date: _____