Maine Office of Marijuana Policy (OMP)
Confidentiality & API User Agreement

1. PARTIES

This Confidentiality and API User Agreement ("Agreement") is made as of this _____day of_____20_____ ("Effective Date") by and between __ ("Provider") and the Maine Office Of Marijuana Policy ("State") (collectively the "Parties"), regarding the provision of one or more secondary software systems ("System," as further defined below) to one or more licensed or registered marijuana establishment(s) authorized by the State to operate an adult use or medical marijuana business in the State of Maine ("Licensee or Registrant"). The Provider and the State hereby agree to the following terms and conditions; any stipulations or modifications to this Agreement shall be clearly indicated herein, must be attached to this Agreement, where applicable, and executed contemporaneous to the execution of this Agreement.

2. EFFECTIVE DATE AND NOTICE OF NONLIABILITY

The Agreement shall not be effective or enforceable until it is approved and signed by all Parties.

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 or Registrant for any reason, including but not limited to the purpose of reimbursing Provider or any Licensee or Registrant for any payments or expenses Provider or any Licensee or Registrant may make or incur, including, without limitation, any such payments or expenses made or incurred pursuant to any agreement between Provider and any Licensee or Registrant. Nor shall any provision in this Agreement be construed as imposing liability on the State for any expenses Provider or Licensee or Registrant may incur or otherwise make in connection with this Agreement or the performance of this Agreement. Provider shall indemnify and hold harmless the State and its officers, agents, and employees from and against any and all claims, liabilities, and costs, including reasonable attorney fees, for any and all injuries to persons or property or claims for money damages, including for violation of intellectual property rights, arising from the negligent acts or omissions of the Provider, its employees or agents, officers or Subcontractors in performance of work or provision of services under 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

A Licensee or Registrant is required to use the inventory tracking system

developed by the State, currently known as METRC, as the exclusive inventory tracking system of record. Licensees and Registrants are also permitted to use a Provider's System to access and input required inventory tracking data into METRC. Licensees and Registrants 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, Registrant and qualified patient information shall be held strictly confidential. The State has agreed to permit Licensees and Registrants 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 into and complies with this Agreement to protect the confidentiality, security and integrity of the information and data contained in METRC. The Provider herein agrees to maintain data integrity and confidentiality, 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 inventory tracking system vendor assigned by the State, METRC.

b. "API Key" means an alphanumeric code generated through and owned by 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:

   i. "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) or Registrant(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) or Registrant(s).

   ii. "User API Key" means an API Key that is specific to a particular Licensee or Registrant, which only such Licensee or Registrant is able and authorized to generate, obtain, and/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 or Registrant's METRC account and allows access to that Licensee or Registrant's METRC data and information.

c. "Data Breach" or "Breach" means, unless context indicates otherwise, the actual accidental or deliberate disclosure of or access to Confidential Information to a person who is not authorized to have access to it.

d. "Incident" means an accidental or deliberate event that results in or poses a threat of 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, (v) changes to the State's system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent, (vi) a Data Breach, or any other failure to comply with the State's Information Security Policy.

e. "Licensee" means a natural person or business entity licensed by the State pursuant to 28-B MRS, ch. 1 and 18-691 CMR, ch. 1, to operate a marijuana establishment.

f. "METRC" or "METRC system" means the marijuana inventory tracking system developed to enable the State to track and trace all legally grown marijuana from immature plant to sale or transfer to patients or adult consumers, and also includes any successor inventory tracking system that the State permits or requires Licensees and Registrants 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) protected health information (PHI), (ix) social security number, (x) driver's license number, (xi) individual identification card number, (xii) registry identification card or registration certificate number, or (xiii) any other information that identifies an individual personally.

i. "Protected Health Information (PHI)" means personal health information protected from unauthorized disclosure or transmission pursuant to the HIPAA Privacy Rule, 45 CFR Parts 160 and 164, Subparts A and E.

j. "Provider" means a 3rd Party Vendor working with an OMP Licensee or Registrant. In the event that a Licensee or Registrant develops its own secondary software system to interface with METRC, it is a "Provider" for the purposes of this Agreement, and its privileges and obligations as a Provider are governed by this Agreement.

k. "Provider Agreement" means an agreement between a Licensee or Registrant and Provider entered into for the purpose of providing a System or Services to the Licensee or Registrant.

l. "Registrant" means any registered caregiver, registered dispensary, registered marijuana testing facility, registered manufacturing facility, or inherently hazardous substance registrant that is registered by the State pursuant to 22 MRS, ch. 558-C and 18-691 CMR,

ch. 2.

m. "Services" means the services to be performed by Provider to a Licensee or Registrant pursuant to the Provider Agreement in connection with the provision, operation or maintenance of the System.

n. "Subcontractor" means any third party engaged by Provider to aid in performance of Provider's obligations to Licensee(s) and/or Registrant(s).

o. "System" means the secondary software system provided by Provider for use by a Licensee or Registrant. Such Systems may be used to collect information to be used by the Licensee or Registrant in operating their businesses, including, but not limited to, secondary inventory tracking and point of sale systems.

5. CONFIDENTIAL INFORMATION

a. "Confidential Information" includes, but is not limited to:
   i. "Personally identifiable information (PII)" which includes, but is not limited to, the full name, or first initial and last name, of any individual who is an owner, employee, consumer or patient of a Licensee or Registrant; any individual's Social Security Number; any individual's date of birth; any individual's home address; any individual's electronic mail (e-mail) address; and/or any other owner, employee, consumer or qualified patient contact information;
   ii. "Financial information" which includes, but is not limited PCI data; payment information; inventory information; transactional data; and/or bank or other financial institution account information;
   iii. Protected Health Information (PHI); and
   iv. Any other data collected by and maintained by the State in METRC.

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 by the recipient of the request.
c. Any unauthorized access or attempt to gain unauthorized access to any Confidential Information shall be promptly reported to the State in all instances and to any affected individual as required by and in accordance with State or Federal law.
d. The State reserves the right to move to quash any subpoena received from a third party seeking Confidential Information.

6. AUTHORIZATION

a. By executing this agreement, the State hereby authorizes METRC to provide a Vendor API Key to Provider to be used in combination with a Licensee or Registrant's User API Key to furnish Provider access to data contained within the METRC system which the Licensee or Registrant is authorized to view or retrieve. This API key is used for the purposes of

communicating real-time sales and/or inventory information to the METRC system. The authorization is granted for use by Licensee(s) or Registrant(s) in operating the business of such Licensee(s) or Registrant(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 Agreement grants Licensee or Registrant 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-me.metrc.com/documentation#getting-started.

b. Provider hereby agrees that a Licensee or Registrant may, at its sole discretion block a Provider's access to its data in METRC by deactivating such Licensee or Registrant's User API Key and generating a new one or having METRC generate a new User API Key.

c. Provider hereby agrees that a Licensee or Registrant is solely responsible for ensuring all transactions and inventory adjustments are accurately represented in the METRC system. Daily verification of reconciliation should occur to ensure proper reporting. Provider acknowledges that upon request by the State, a Licensee or Registrant shall provide the State with reporting verification that all transactions have been reconciled; and Provider agrees to ensure their System can provide such reporting verification to Licensee or Registrant.

d. Provider acknowledges that Licensees and Registrants will have their User API key revoked if transactions and/or inventory adjustments are not accurately represented in the METRC system. Provider agrees that notwithstanding any contrary provision in a Provider Agreement, and in keeping with any obligation of the State to maintain the confidentiality, security and integrity of all data and information in the METRC system, Provider expressly waives, and shall not be entitled to seek or obtain, injunctive, equitable or other relief against the State or METRC to compel the furnishing of any Licensee or Registrant's User API Key to Provider. Provider agrees that a Licensee or Registrant shall maintain, at all times, the right to terminate the Provider Agreement or otherwise discontinue use of Provider's System and Services.

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

f. Provider agrees that 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 in this Agreement.

g. Any Provider executing this Agreement is subject to all State laws, regulations, and any other rules defining the integrity and accuracy of data entered into the State's inventory tracking system (METRC). Information entered into the system inaccurately or in violation of the State law, regulation or any other rule could result in the State's revocation of the Provider's Vendor API key.

h. Provider acknowledges that misrepresentation or knowingly entering false information into the State's tracking system will result in the revocation of its 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-me.metrc.com/documentation#getting-started

i. Provider acknowledges that API keys are non-transferable and cannot be shared. Provider acknowledges that sharing an API key with any entity outside of Provider's 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. Transactional data is required to be entered into METRC via the user interface (UI), API, or any other means in real-time or as close as possible to real-time.

7. SECURITY REQUIREMENTS

a. The Provider agrees to abide by all applicable Federal, State and local laws concerning information security. Provider expressly agrees to be bound by and to comply with all applicable State of Maine IT policies, standards, and procedures, posted at https://www.maine.gov/oit/policies/ and any subsequent amendments. This includes, but is not limited to, the Digital Accessibility and Usability Policy, Information Security Policy, and Information Privacy Policy. Provider shall routinely review and must at all times comply with all applicable State of Maine IT policies, standards and procedures.

b. Provider shall limit access to and possession of Confidential Information to only employees whose responsibilities reasonably require such access or possession and shall train such employees on the Confidentiality obligations set forth herein.

c. Provider shall protect Confidential Information 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. 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, including, without limitation, any unauthorized disclosure of Confidential Information, or other event requiring notification under applicable law, the Provider agrees to assume responsibility for informing all such individuals in accordance with applicable law; 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; and to otherwise assume all liability for any correction or repair required due to the Provider's failure to protect Confidential Data.

d. Provider shall disclose all of its non-proprietary security processes and technical limitations to the State. Provider shall, upon demand by the State, provide documentation or otherwise demonstrate compliance with all security requirements contained in this Agreement to State's satisfaction, including, where appropriate, disclosure of otherwise proprietary information.

8. SECURITY INCIDENT OR DATA BREACH RESPONSE AND NOTIFICATION

a. Provider shall inform the State of any security incident or data breach, including, without limitation, when any Provider System that accesses, processes or stores State data or State systems is subject to unintended or otherwise unauthorized access or attack. Unintended or otherwise unauthorized 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.

b. Provider 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 OMP's Director of Data Analytics.

c. Provider agrees to notify the State within two (2) hours if there is a threat to Provider's System or Services as it pertains to the use, disclosure, and security of the State data.

d. Provider agrees that if an unauthorized use or disclosure of any Confidential Data occurs, the Provider shall provide written notice to the State within one (1) business day after Provider's discovery of such use or disclosure and thereafter all information the State requests concerning such unauthorized use or disclosure.

e. Provider, within one day of discovery, shall report to the State any improper or non-authorized use or disclosure of Confidential Information. Provider's report shall identify:

   i. the nature of the unauthorized use or disclosure;
   ii. the Confidential Information used or disclosed,
   iii. who made the unauthorized use or received the unauthorized disclosure;
   iv. what the Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure;
   v. what corrective action the Provider has taken or shall take to prevent future similar unauthorized use or disclosure; and
   vi. Provider shall provide such other information, including a written report, as reasonably requested by the State.

f. Incident Response: The Parties acknowledge that Provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Agreement. Disclosure and discussion of security incidents with the State should be handled on an urgent basis, as part of Provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the Agreement.

g. Security Incident Reporting Requirements: Provider shall immediately report a security incident to the OMP Director of Data Analytics.

h. Data Breach Reporting Requirements: If Provider has actual knowledge of a confirmed data breach that affects the confidentiality or security of any Confidential Information that is subject to applicable data breach notification law, for example, PHI and PCI, or special

confidentiality protection, such as trade secrets, the Provider shall (1) promptly notify the OMP Director of Data Analytics 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.

i. Data Breach Responsibilities
   i. This section only applies when a data breach occurs with respect to Confidential Information within the possession or control of the Provider.
   ii. 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 data breach.
   iii. 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.

j. Unless otherwise stipulated, if a data breach is a direct result of the Provider's breach of its obligation to encrypt Confidential Information 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 or federal 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.

9. DATA PROTECTION

a. Data Ownership
   The State will own all right, title and interest in Confidential Information that is related to the services provided by 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 Agreement or (4) at the State's written request.
b. Loss of Data
   In the event of loss of any Confidential Information 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 OMP. The Provider shall ensure that all data is backed up and is recoverable by the Licensee or Registrant. 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 Confidential Information 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 Confidential Information at any

time. To this end, the Provider shall safeguard the confidentiality, integrity and availability of Confidential Information and comply with the following conditions:

i. 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.

ii. 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 Agreement shall become and remain property of the State.

iii. Unless otherwise stipulated, the Provider shall encrypt all Confidential Information at rest and in transit, to the level of protection and encryption identified and made a part of this Agreement.

iv. 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.

v. The Provider shall not use any information collected or created in connection with the service issued under this Agreement 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, Licensee, or Registrant. This includes the ability for the State to import or export data to/from third parties, and to monitor any transaction in real time.

c. Encryption of Data at Rest

The Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in Federal Information Processing Standards (FIPS), FIPS 140-2, Security Requirements for Cryptographic Modules for all Confidential Information, unless

the State approves in writing, the storage of Confidential Information on a Provider portable device in order to accomplish Agreement work.

d. Encryption of Data in Transit
The Provider shall ensure that all data transmissions adhere to government server requirements as outlined in National Institute for Standards and Technology (NIST) Special Publication (SP), NIST SP 800-52 Rev.2, or subsequent revisions which supersede its predecessors. This includes the requirement that all Transport Layer Security (TLS) servers and clients support TLS 1.2 configurations with FIPS-based cipher suites, and that support for TLS 1.3 be added by January 1st, 2024. All vulnerable versions of protocols, including but not limited to TLS v 1.0 and 1.1, must be explicitly blocked. All current NIST guidance regarding certificates, TLS extensions, and protocols must be adhered to.

11. REMEDIES

The Parties agree that 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 for cause or breach 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.

b. 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 and Provider shall certify that no copies of Confidential Information remain in the possession or control of Provider.

c. 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 any 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.

d. 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.

The Parties further agree the State may, at its sole discretion, exercise the following remedies at any time.

a. Early Termination in the Public Interest or to protect the confidentiality, security or integrity of the METRC system.
    i. If this Agreement ceases to further the public policy of the State, or to protect the confidentiality, security, or integrity of the METRC system, 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.
    ii. All Confidential Information in the possession or control of Provider shall be immediately returned to the State and Provider shall certify that no copies of Confidential Information remain in the possession or control of Provide

b. 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:
    i. 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.
    ii. 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. 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 immediately contact the State upon receipt of any court orders, subpoenas, discovery, litigation holds, discovery searches and requests for expert testimony related to the State's data (Confidential Information) under this Agreement, or which in any way might reasonably require access to the data of the State. The Provider shall not respond to subpoenas, service of process and other legal requests related to the State's data without first notifying the State and permitting the State to respond.

13. MAINE LAW PREVAILS

This Agreement shall be construed, interpreted, and enforced according to the laws of the State of Maine. Provider agrees to submit to the Jurisdiction of Maine. 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

By signing this Agreement Provider acknowledges that it has 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

This Agreement represents the entire agreement of the parties. Additions, deletions, or other changes hereto shall not have any force or effect unless expressed in writing and signed by both parties. 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 provisions of Sections 2 and 5-13 shall survive the termination or expiration of this agreement

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: _____

Maine Office of Marijuana Policy

Print Name: _____

Title: _____

Email: _____

Phone #: _____

Signature: _____

Date: _____