# STATE OF MONTANA, DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES METRC APPLICATION PROGRAMMING INTERFACE CONFIDENTIALITY & USER AGREEMENT

This is an agreement between the Third party point of sale software vendor as signed below and the State of Montana Department of Public Health and Human Services in which the Third party point of sale software vendor hereby agrees to the following terms and conditions.

## 1. DEFINITIONS

### A. API

"API" means the Application Programming Interface designed, developed, and maintained by Franwell, or any successor organization.

### B. API Key

"API Key" means an alphanumeric code generated through METRC to gain programmatic access to METRC and automatic electronic communication of data and information between Third party point of sale software vendor's System and METRC. There are two kinds of API Keys:

#### i. Vendor API Key

"Vendor API Key" means an API Key that is specific to Third party point of sale software vendor and Third party point of sale software vendor's System, which must be used by every instance of Third party point of sale software vendor'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 Third party point of sale software vendor's System and METRC pertaining to such Licensee(s).

#### ii. User API Key

"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. Confidential Information**

"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 or data concerning individuals and Licensees including financial information such as banking information and social security numbers, which has been communicated, furnished, or disclosed by the State to Third party point of sale software vendor. Confidential information includes but is not limited to any information obtained by Third party point of sale software vendor through the interface between the METRC system and the System. Confidential Information may also include any information disclosed to Third party point of sale software vendor 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 marijuana or marijuana product, if such data, reports, or records are or are intended to be provided to the State through the METRC system or otherwise; **(vii)** business plans and performance related to the past, present or future activities of such party, its affiliates, subsidiaries and affiliated companies; **(viii)** all types of Licensee data, including but not limited to, names and lists of other license holders, service third party point of sale software vendors, 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.

**E. Franwell**

"Franwell" means Franwell, Inc., the company engaged by the State of Montana Department of Public Health and Human Services to design,

develop, provide, host and maintain the Department's METRC system, and also includes any successor organization.

**F. Incident**

"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; **(iii)** the unauthorized use of METRC for the processing or storage of data; **(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.

**G. Licensee**

"Licensee" means a person holding a license issued under MCA 50-46-301 et.seq.

**J. METRC**

"METRC" or "METRC system" means the marijuana inventory tracking system developed by Franwell to enable the department to track all legally grown marijuana from seed to sale, and also includes any successor inventory tracking system that the department permits or requires Licensees to utilize.

**K. PCI Data**

"PCI Data" means payment card information data. That is, 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.

**L. PII Data**

"PII Data" means personally identifiable information. That is, information about an individual collected by the State or any other governmental entity that could reasonably be used to identify such individual including but not limited to that contemplated by 50-16-502 and 30-14-1704 MCA. Personally identifiable information 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.

**M. Third party point of sale software vendor**
"Third party point of sale software vendor" means a third-party system third party point of sale software vendor approved by the department to integrate with the statewide monitoring system.

**N. Third party point of sale software vendor Contract**
"Third party point of sale software vendor Contract" means an agreement between a Licensee and Third party point of sale software vendor entered into for the purpose of providing a System or Services to the Licensee.

**O. Services**
"Services" means the services to be performed by Third party point of sale software vendor to Licensee pursuant to the Third party point of sale software vendor Contract in connection with the provision, operation or maintenance of the System.

**P. State**
"State" means the State of Montana Department of Public Health and Human Services and the various agencies that are involved in the implementation, maintenance and oversight of the medical marijuana program in accordance with the Montana Medical Marijuana Act (MCA 50-46- 301 et. seq.) and the related Administrative Rules of Montana. These agencies include but are not limited to the Department of Revenue; Department of Agriculture and the Department of Health and Human Services.

**Q. Subcontractor**
"Subcontractor" means any third party engaged by Third party point of sale software vendor to aid in performance of Third party point of sale software vendor's obligations to Licensee(s).

**R. System**
"System" means the secondary software system provided by Third party point of sale software vendor 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.

## 2. EFFECTIVE DATE AND NOTICE OF NONLIABILITY

The Third party point of sale software vendor hereby agrees the Agreement shall not be effective or enforceable until it is approved by the State. 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, Third party point of sale software vendor or any Licensee for any reason, including but not limited to the purpose of reimbursing Third party point of sale software vendor or Licensee for any payments or expenses Third party point of sale software vendor or any Licensee may make or incur, including, without limitation, any such payments or expenses made or incurred pursuant to any contract between Third party point of sale software vendor and any Licensee. Nor shall any provision in this Agreement be construed as imposing liability on the State for any expenses Third party point of sale software vendor or Licensee may make or incur in connection with this Agreement or the performance of this Agreement. Third party point of sale software vendor expressly waives any claims asserting liability against State in connection with this Agreement or the performance of this Agreement.

## 3. RECITALS

### A. Authority and Approval

Authority to enter into this Agreement is based on 50-46-301 et. seq.

### B. Consideration

The Third party point of sale software vendor acknowledge that the mutual promises and covenants contained herein and other good and valuable consideration are sufficient and adequate to support this Agreement.

### C. Purpose

Licensees are required to interface with the inventory tracking system developed by the State, currently known as METRC, as the primary inventory tracking system of record. Licensee information in METRC is confidential and is exempt from disclosure under 50-16-501 et. seq. and 50-16-603 MCA. The State has agreed to permit Licensees to communicate information electronically to and from METRC through Third party point of sale software vendor's System or Services via an API, but this permission is

valid only if the Third party point of sale software vendor of the System enters an agreement to protect the confidentiality of the information/data contained in METRC and the integrity of METRC's design and processes, and to comply with the security requirements and standards set forth below.

**4. AUTHORIZATION**

The State authorizes Franwell to provide a Vendor API Key to Third party point of sale software vendor, which, when used in combination with a Licensee's User API Key which the Licensee may furnish to Third party point of sale software vendor, permits Third party point of sale software vendor's System to access the API for the purposes of communicating information to the METRC system, and retrieving such information from the METRC system, for use by Licensee(s) in operating the business of such Licensee(s). This Agreement, and Third party point of sale software vendor'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.

The Vendor API Key shall permit Third party point of sale software vendor's System with access to the API only if the Vendor API Key is used in combination with the User API Key. A Licensee that contracts with Third party point of sale software vendor for use of Third party point of sale software vendor's System may furnish Third party point of sale software vendor with its User API Key to grant access to the API. The Third party point of sale software vendor agrees that it is not authorized to share a User API Key with other entities without permission from the State or a Licensee. The Third party point of sale software vendor acknowledges that the State or a Licensee shall have the right to block Third party point of sale software vendors' access to Licensee's METRC data by deactivating such Licensee's User API Key and generating, or having Franwell generate, a new User API Key through METRC. If the State deactivates the Vendor API Key as described under section 5, the User API Key is also deactivated and a new User API Key must be generated.

The Third party point of sale software vendor agrees that notwithstanding any contrary provision in a Third party point of sale software vendor Contract, and in keeping with the State's obligation to maintain the confidentiality of Licensee(s) data and information, Third party point of sale software vendor 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 Third party point of sale software vendor.

The Third party point of sale software vendor agrees that the Licensee shall maintain at all times the right to terminate the Third party point of sale software vendor Contract or otherwise discontinue use of Third party point of sale software vendor's System and Services. The Third party point of sale software vendor further agrees to operate in good faith and with fair dealing at all times when providing a System or Services that interface with the METRC system.

## 5. CONFIDENTIALITY

Third party point of sale software vendor shall comply with and shall cause each of its agents, employees, Subcontractors, permitted assigns and any other individual or entity assisting with Third party point of sale software vendor's provision of a System or Services to Licensee to comply with the provisions of this section if that person will or may have access to Confidential Information in connection with its performance, which obligations shall survive the termination of this Agreement.

### A. Confidentiality

Third party point of sale software vendor shall keep all Confidential Information confidential at all times, to ensure compliance with all laws and regulations concerning confidentiality of confidential information including but not limited to that contemplated by 50-16-501 MCA et.seq and 50-46-603 MCA. Any request or demand, including subpoenas, by a third party for confidential information in the possession or control of third party point of sale software vendor shall be immediately forwarded to the State's principal representative 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 in the possession or control of third party point of sale software vendor, whether the subpoena is directed to third party point of sale software vendor or the State. Third party point of sale software vendor agrees to cooperate with the State, if requested, in proceedings related to any motion to quash a subpoena, at no expense to the State.

### B. Notification

Third party point of sale software vendor shall provide its agents, employees, subcontractors, and permitted assigns who will or may come into contact with confidential information with a written explanation of the

confidentiality requirements herein, to which they are subject, prior to permitting any such individual to access such Confidential Information.

**C. Protection**

Third party point of sale software vendor is responsible for the protection and security of all confidential information provided to it by the State or which is accessible using the API Key. If Third party point of sale software vendor provides physical or logical storage, processing or transmission of, or retains, stores, or is given, confidential information, third party point of sale software vendor shall, and shall cause its agents, employees, subcontractors, and permitted assigns to, **(i)** provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this agreement; **(ii)** maintain network, system, and application security, which includes, but is not limited to, network firewalls, intrusion detection (host and network), and annual security testing; **(iii)** comply with State and federal regulations and guidelines related to overall security, confidentiality, integrity, availability, and auditing; **(iv)** ensure that security is not compromised by unauthorized access to computers, program, software, databases, or other electronic environments; and **(v)** report all Incidents immediately, and all attempted incidents on an annual basis to the State.

Third party point of sale software vendor shall provide the State with access, subject to third party point of sale software vendor's reasonable access security requirements, seven (7) days a week, twenty-four (24) hours a day, for the purpose of inspecting and monitoring access and use of confidential information and evaluating physical and logical security control effectiveness. As set forth in section 2 of this agreement, the State shall not be responsible for any expenses incurred in connection with this agreement, including, but not limited to, third party point of sale software vendor's expenses related to compliance with this section.

**D. Use, Information Security Compliance, and Retention**

Third party point of sale software vendor expressly agrees to be bound by and to comply with the State of Montana security policies, standards and procedures. Third party point of sale software vendor shall routinely review such statutes, rules, policies, standards and guidelines.

Third party point of sale software vendor shall cooperate, and shall cause its Subcontractors to cooperate, with the performance of a security audit conducted by the State.

Confidential Information of any kind shall be stored, processed, or transferred only in or to facilities located within the United States, and shall not be distributed or sold to any third party, retained in any files or otherwise, or used by Third party point of sale software vendor or its agents in any way, except as authorized by this Agreement, by law, unless approved in writing by the Montana Department of Public Health and Human Services. Third party point of sale software vendor shall provide and maintain a secure environment that ensures confidentiality of all Confidential Information wherever located. Neither Third party point of sale software vendor nor any of its agents, employees, Subcontractors, or permitted assigns shall have any rights to use or access any data or information of any Montana state agency, except with the prior written approval of the State.

**E. Incident Notice**

If Third party point of sale software vendor becomes aware of an Incident involving any Confidential Information, it shall notify the State immediately and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, if any. Unless Third party point of sale software vendor establishes that neither Third party point of sale software vendor nor any of its agents, employees, Subcontractors, or permitted assigns was the cause or source of the Incident, Third party point of sale software vendor shall be responsible for the cost of notifying each person whose Confidential Information may have been compromised by the Incident. The State will own all right, title and interest in its data that is related to the services provided by this Agreement.

**F. Incident Remediation**

Third party point of sale software vendor, at its sole cost, shall be responsible for determining the cause of an Incident, and for producing a remediation plan to reduce the risk of a similar Incident in the future. Third party point of sale software vendor shall present its analysis and remediation plan to the State within ten (10) days of notifying the State of an Incident. The State reserves the right to adjust this plan, in its sole discretion. If Third

party point of sale software vendor cannot produce its analysis and plan within the allotted time, the State, in its sole discretion, may perform such analysis and produce a remediation plan, and Third party point of sale software vendor shall timely reimburse the State for the reasonable costs thereof.

**G. Incident Liability**

Disclosure of Confidential Information by Third party point of sale software vendor or any of its agents, employees, Subcontractors, or permitted assigns for any reason may be cause for legal action by third parties (including Licensee(s)) against Third party point of sale software vendor, the State, or their respective agents. Third party point of sale software vendor shall indemnify, save, and hold harmless the State, its employees, and agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred as a result of any act or omission by Third party point of sale software vendor, or its employees, agents, Subcontractors, or assignees pursuant to this Agreement. Notwithstanding any other provision of this Agreement, Third party point of sale software vendor shall be liable to the State for all direct, consequential and incidental damages arising from an Incident caused by Third party point of sale software vendor or its agents, employees, Subcontractors, or permitted assigns.

**H. End-of-Agreement Data Handling**

Upon request by the State made before or within sixty (60) days after the effective date of termination of the Agreement, Third party point of sale software vendor will make available to the State a complete and secure download file of all data, including, but not limited to, all Confidential Information, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in their native format. All such data shall be encrypted and appropriately authenticated. The Third party point of sale software vendor agree that on the termination of the provision of Services, Third party point of sale software vendor shall, at the choice of the State, return all Confidential Information in the possession or control of the Third party point of sale software vendor, and the copies thereof, to the State, or Third party point of sale software vendor shall destroy all such Confidential Information and certify to the State that it has done so. If legislation imposed upon Third

party point of sale software vendor prevents it from returning or destroying all or part of the Confidential Information in the possession or control of Third party point of sale software vendor or obtained through the API, Third party point of sale software vendor warrants that it will guarantee the confidentiality of all Confidential Information in the possession or control of Third party point of sale software vendor or obtained through the API and will cease any activity that processes or otherwise utilizes such data.

**I. Disposition of Data**

The State retains the right to use the System to access and retrieve Confidential Information stored on Third party point of sale software vendor's infrastructure at the State's sole discretion. Third party point of sale software vendor warrants and shall cause each Subcontractor to warrant that upon request of the State, Third party point of sale software vendor or such Subcontractor shall submit its data processing facilities for an audit of its compliance with section 5, including but not limited to the measures referred to in section 5(D). The State reserves its rights, title, and interest, including all intellectual property and proprietary rights, in and to METRC, METRC system data, confidential information, and all related data and content.

**J. Safeguarding PII Data**

If Third party point of sale software vendor or any of its agents, employees, Subcontractors, and permitted assigns will or may receive PII Data under this Agreement, Third party point of sale software vendor shall provide for the security of such PII Data, in a form acceptable to the State, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, and audits. Third party point of sale software vendor shall take full responsibility for the security of all PII Data in its possession or in the possession of its agents, employees, Subcontractors, or permitted assigns, and shall hold the State harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof.

**K. Safeguarding PCI Data**

If Third party point of sale software vendor or any of its agents, employees, Subcontractors, and permitted assigns will or may receive PCI Data under this Agreement, Third party point of sale software vendor shall provide for

the security of the PCI Data, in accordance with Data Security Standard (DSS). Security safeguards shall include, without limitation, supervision by responsible employees, approval of Subcontractors as required by State or federal law, non-disclosure of information other than as necessary in the performance of Third party point of sale software vendor's or Subcontractor's obligations under this Agreement, non-disclosure protections, proper accounting and storage of information, civil and criminal penalties for non-compliance as provided by law, certifications, and inspections.

L. A violation of this section or agreement including the failure to report or notify the State of any incident may result in the deactivation or revocation of the Vendor API Key.

## 6. BREACH

### A. Defined

In addition to any breaches specified in other sections of this Agreement, the failure of Third party point of sale software vendor to perform any of its material obligations hereunder in whole or in part or in a timely and satisfactory manner constitutes a breach. The institution of proceedings under any bankruptcy, insolvency, reorganization, or similar law, by or against Third party point of sale software vendor, or the appointment of a receiver or similar officer for Third party point of sale software vendor or any of its property, which is not vacated or fully stayed within twenty (20) days after the institution or occurrence thereof, shall also constitute a breach. Breach also shall occur upon Third party point of sale software vendor's unauthorized use, disclosure or retention of Confidential Information. Third party point of sale software vendor shall, within 24 hours, provide the State with written notice of the institution of proceedings under any bankruptcy, insolvency, reorganization, or similar law, by or against Third party point of sale software vendor, or the appointment of a receiver or similar officer for Third party point of sale software vendor or any of its property.

### B. Notice and Cure Period

In the event of a breach, notice of such shall be given in writing by the aggrieved party to the other party by hand-delivery with receipt required or sent by certified or registered mail to such party's principal representative at

the address set forth below. If sent by certified or registered mail, notice shall be deemed received two business days after the date of mailing as reflected on the postmark. In addition to but not in lieu of a hard-copy notice, notice also may be sent by email to the e-mail addresses, if any, as set forth below. Any Party may from time to time designate by written notice substitute addresses or persons to whom such notices shall be sent.

**i. State:**

| |
|---|
| Director's Office , Department of Health and Human Services Medical Marijuana Program |
| P.O. Box 4210<br>Third Floor Sanders Building |
| Helena, MT 59604 |

**ii. Third party point of sale software vendor:**

| |
|---|
| Name and title of person: |
| Company Name: |
| Address: |
| Email address: |

If such breach is not cured within thirty (30) days of receipt of written notice, or if a cure cannot be completed within thirty (30) days, or if cure of the breach has not begun within thirty (30) days and pursued with due diligence, the State may exercise any of the remedies set forth in section 7.

**C. Deactivation**

Notwithstanding any provision to the contrary herein, the State, in its sole discretion, need not provide advance notice or a cure period and may immediately deactivate Third party point of sale software vendor's Vendor

API Key if the State determines such action is warranted to maintain the confidentiality of Confidential Information as required in section 1.C and this agreement.

## 7. REMEDIES

If Third party point of sale software vendor is in breach under any provision of this Agreement, the State shall have all of the remedies listed in this section 7.A in addition to all other remedies set forth in other sections of this Agreement following the notice and cure period set forth in section 6.B. 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. Third party point of sale software vendor shall continue performance of this Agreement to the extent not terminated, if any.

#### i. Obligations and Rights

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

#### ii. Vendor API Key Deactivation

Irrespective of any period set forth in section 6.B, immediately upon any breach of this Agreement, the State may deactivate Third party point of sale software vendor's Vendor API Key. **Third party point of sale software vendor agrees that the Vendor API Key does not constitute a license and expressly waives any rights associated with the provision of a license in Montana. Third party point of sale software vendor specifically agrees it has no right to a**

**hearing or other legal or administrative process regarding the deactivation of the Vendor API Key.**

**iii. Damages**

Notwithstanding any other remedial action by the State, Third party point of sale software vendor shall remain liable to the State for any damages sustained by the State by virtue of any breach under this Agreement by Third party point of sale software vendor.

**B. Early Termination in the Public Interest**

The State is entering into this Agreement for the purpose of carrying out the public policy of the State of Montana, as determined by its Governor, Legislature, and/or Courts. If this Agreement ceases to further the public policy of the State, the State, in its sole discretion, may deactivate Third party point of sale software vendor'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.

**i. Obligations and Rights**

Upon receipt of notice of breach, Third party point of sale software vendor shall be subject to and comply with the same obligations and rights set forth in section 7.A.i.

**C. 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. Removal**

Notwithstanding any other provision herein, the State may demand immediate removal of any of Third party point of sale software vendor'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. Intellectual Property**

If Third party point of sale software vendor infringes on a patent, copyright, trademark, trade secret, or other intellectual property right while performing the services or providing the System, Third party

point of sale software vendor 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.

## 8. OTHER PROVISIONS

### A. Indemnification

Third party point of sale software vendor shall indemnify, save, and hold harmless the State, its employees, and agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred as a result of any act or omission by Third party point of sale software vendor, or its employees, agents, Subcontractors, or assignees pursuant to the terms of this Agreement; however, the provisions in this Agreement shall not be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Montana Medical Marijuana Act (MCA 50-46-301 et.seq.) and the related Administrative Rules of Montana Revised Statutes, as now or hereafter amended.

### B. Jurisdiction and Venue

All suits or actions related to this Agreement shall be filed and proceedings held in the State of Montana, County of Lewis and Clark.

### C. Governmental Immunity

Liability for claims for injuries to persons or property arising from the negligence of the State of Montana, its departments, institutions, agencies, boards, officials, and employees is controlled and limited by the provisions of the Montana Code Annotated and related immunity authorities, as applicable now or hereafter amended. No term or condition of this Agreement shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protections, or other provisions, of the Montana Code Annotated and related immunity authorities. The Third party point of sale software vendor agrees that the State retains all such immunities, rights, benefits, and protections.

**D. Choice of Law**

This Agreement shall be construed, interpreted, and enforced according to the laws of the State of Montana. Montana law, and rules and regulations issued pursuant thereto, shall be applied in the interpretation, execution, and enforcement of this Agreement. Any provision included or incorporated herein by reference which conflicts with said laws, rules, and regulations shall be null and void. Any provision incorporated herein by reference which purports to negate this or any other provision in whole or in part shall not be valid or enforceable or available in any action at law, whether by way of complaint, defense, or otherwise. Any provision rendered null and void by the operation of this provision shall not invalidate the remainder of this Agreement, to the extent capable of execution.

**E. Binding Arbitration Prohibited**

The State does not agree to binding arbitration by any extra-judicial body or person. Any provision to the contrary in this Agreement or incorporated herein by reference shall be null and void.

**F. Employee Financial Interest/Conflict of Interest.**

The signatories aver that to their knowledge, no employee of the State has any personal or beneficial interest whatsoever in the System or Services described in this Agreement. Third party point of sale software vendor has no interests and shall not acquire any interest, direct or indirect, that would conflict in any manner or degree with the performance of Third party point of sale software vendor's Services and Third party point of sale software vendor shall not employ any person having such known interests.

**G. Entire Understanding**

This Agreement represents the complete integration of all understandings between the Third party point of sale software vendor and the State, 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.

Facsimile and Portable Document Format ("PDF") copies of the Third party point of sale software vendor's signatures shall be treated as originals.

The Third party point of sale software vendor has caused their duly authorized representatives to execute this Agreement as of the date set forth above. The Third

party point of sale software vendor hereby agrees to all the foregoing terms and conditions.

Third party point of sale software vendor:
_____

Signature: _____

Print name: _____

Title: _____

State Authorizer:  Darci Wiebe

Signature: _____

Title: Bureau Chief, Montana Medical Marijuana Program

Effective Date: _____