Security

Policies and procedures for identifying, recording, and reporting diversion, theft, or loss, and for correcting all errors and inaccuracies in inventories.

Employee security policies, including personal safety and crime prevention techniques
Security for employees at our Marijuana Establishment facilities will be established through perimeter and interior monitoring, a restrictive ID/badge system, and limited access area partitioning, and rigorous personnel safety training.

The exterior of the facilities will be well-lit and equipped with video surveillance cameras. Feeds from multiple exterior (and interior) viewing angles will be available. Interior cameras will be installed in all limited access areas and locations at which product is stored, received, weighed, handled, and provisioned to patients and adult use consumers. The video recording equipment will be securely stored in a security closet in a limited access room that only authorized Executive Management Team (EMT) members can access.

Only registered Marijuana Research Facility Agents, persons authorized by the state regulations and subject to the requirements of the state regulations outside vendors, contractors, and visitors, will be allowed access to the Marijuana Establishment. All ID's for visitors will be verified via ID card scanner or the state ID reference book.

RFID access cards will be used to control movement throughout the facilities. All employees will be assigned an ID/access card consistent with their security level and access permissions. State issued ID cards will be used as the employee identification card and will be printed with the employee's name, picture, and employee number. ID/access cards must be visibly worn by every employee at all times. Lost ID/access cards will be reported immediately to Research and Development management. If it was an access card, they will program the card as "lost" in the access control system. If access is attempted by using the lost card in any card reader in the facility, an alarm will go off, with notifications sent to the EMT. If deemed appropriate, law enforcement will be notified by the EMT in this situation. Lost Marijuana Research Facility Agent ID cards will be reported to the Cannabis Control Commission within 5 business days.

Keys will only be issued to management staff and will only be used as a backup for emergency purposes. All building keys and card activation devices will be kept in a limited access location requiring the highest security level to access. Electric locks and card readers will be installed at partitions throughout the facilities. The limited access areas, such as the locked product storage container, will require a RFID identification card to access. The access control systems will record all access events and produce reports specific to each employee, card used, access location, and time and date. Limited access areas shall be accessible to only those employees essential for an efficient operation. Every access point is monitored via cameras.

All authorized vendors, contractors, and visitors will first sign into a visitors' check in system and obtain a visitor ID badge upon entering. They will be escorted at all times by a Marijuana Research Facility Agent authorized to enter limited access areas. The visitor identification badge

must be visibly displayed at all times. All visitors must be logged in and out, and that log will be available for inspection by the Cannabis Control Commission at any time. All visitor ID badges will be returned upon exit.

All staff will be trained in basic safety awareness and additional scenario-specific conduct, as part of their orientation and intensive safety training. In the event of a forced intrusion, staff is instructed to remain calm and not argue, fight, surprise or attempt to use force against an intruder. Staff will comply with demands for products without hesitation. Staff will not in any way hinder the intruder's departure. Employees complete and sign off on confidentiality training that covers the 201CMR17.00 Standards for the Protection of PI of Residents of Commonwealth, M.G.L. c. 93H Security Breaches and HIPAA Privacy Rule.

Corporate Policy Statement

The Occupational Safety and Health Act of 1970 clearly states our common goal of safe and healthful working conditions. The safety and health of our employees continues to be the first consideration in the operation of this business.

Safety and health in our business must be a part of every operation. Without question it is every employee's responsibility at all levels.

It is the intent of this company to comply with all laws. To do this we must constantly be aware of conditions in all work areas that can produce injuries. No employee is required to work at a job he or she knows is not safe or healthful. Your cooperation in detecting hazards and, in turn, controlling them is a condition of your employment. Inform your supervisor immediately of any situation beyond your ability or authority to correct.

The personal safety and health of each employee of this company is of primary importance. The prevention of occupationally induced injuries and illnesses is of such consequence that it will be given precedence over operating productivity whenever necessary. To the greatest degree possible, management will provide all mechanical and physical facilities required for personal safety and health in keeping with the highest standards.

We will maintain a safety and health program conforming to the best management practices of organizations of this type. To be successful, such a program must embody the proper attitudes toward safety and injury and illness prevention not only on the part of supervisors and employees, but also between each employee and his or her co-workers. Only through such a cooperative effort can a safety program in the best interest of all be established and preserved.

Our objective is a safety and health program that will reduce the number of injuries and illnesses to an absolute minimum, not merely in keeping with, but surpassing, the best experience of operations similar to ours. Our goal is nothing less than zero accidents and injuries.

Physical Security Plan

- BASIS: Security at these facilities is paramount. Due to the nature of our business, security is essential to the safe and efficient operation of our business. Many types of

security infractions can affect the operation of this facility. Special attention to security is needed due to the risk and magnitude of harm resulting from the loss of material, misuse of physical assets, or unauthorized access to sensitive areas within this facility.

- GENERAL: This program establishes and defines the components of the Curaleaf Processing Inc. Physical Security Program. This program provides key company personnel with guidelines and standards for physical-security operations to protect employees and assets from damage or loss. To help mitigate the effects of such occurrences Curaleaf Processing Inc. will maintain this plan. This plan is intended to address comprehensively the issues of evaluating and identifying potential threats to our employees and assets, developing written procedures, and communicating information concerning these contingencies to employees.

- RESPONSIBILITY: The Vice President of Security will be solely responsible for all facets of this program and has full authority to make necessary decisions to ensure success of the program. The Northeast Security Team or onsite designee is the sole person authorized to amend these instructions and is authorized to halt any operation of the company where there is danger of security breach.

- Contents of the Physical Security Plan

    1. Written Program.
    2. Program Requirements.
    3. Program Components.
    4. Security Inspections and Surveys.
    5. Security Risk Assessments.
    6. Restricted Areas.
    7. Security Measures.
    8. General Access to Premises.
    9. Policy for Passes and Badges.
    10. Confiscating Passes and Badges.
    11. Access by Local Law Enforcement Agencies.
    12. Keys and Lock Controls (K&LC).

1. *Written Program*. Curaleaf Processing Inc. will review and evaluate this plan under the following conditions:

- On an annual basis.
- When changes occur to applicable regulations.
- When changes occur to local directives.
- When facility operational changes occur.
- When the plan fails.

Effective implementation of this program requires support from all levels of management within this company. This plan will be communicated to all personnel that are affected by it. It

encompasses the total workplace, regardless of number of workers employed or the number of work shifts. It is designed to establish clear goals and objectives.

2. *Program Requirements*. Each level of management has specific responsibilities that allow the program to function effectively. The proper operation of this plan is an integrated process made up of the following components.

- Assessing the threat.
- Assigning specific physical-security duties.
- Conducting security planning.
- Conducting risk analysis.
- Identifying vulnerable areas.
- Designating restricted areas.
- Coordinating security efforts.
- Establishing physical-security councils.
- Employing physical- and procedural-security measures.
- Conducting inspections and surveys.

3. *Program Components*.

- Employee responsibilities
    - Physical security is everyone's responsibility. An effective physical-security program uses an approach that is methodical, deliberate, and ongoing at each management level. Employees at all levels will establish programs that include the components prescribed by this plan. Supervisors will periodically review and be prepared to adjust their programs to the changing threat.

- Assessing the threat.
    - Threat assessments must be developed and updated as necessary.

- Key and lock control.
    - Key and lock control (K&LC) will be designated by the company's The Northeast Security Team or onsite designee. A K&LC matrix will be appointed, filed, and updated as needed by the company's The Northeast Security Team or onsite designee.

- Security planning.
    - The physical security plan will tie security measures together. The plan will integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. The physical security plan must have reasonable and affordable protective measures. Associated costs should be in proportion to the value or criticality of the property being protected and the existing level of risk.

- Risk analysis.
    - Risk analyses are critical to security planning. Risk analyses are used to adapt physical protective measures and security procedures to local conditions. Risk analyses must be

performed on vulnerable areas. Risk analyses will be considered when scheduling follow-on inspections and surveys. Analyses will be kept on file until the next risk analysis is conducted.

- Restricted areas.
    - This company will safeguard assets by declaring high threat areas as restricted, thereby limiting access to that area. Access to restricted areas will be strictly controlled and notices will be posted in plain sight. Violations of restricted areas will be brought to the attention of the security officer and The Northeast Security Team or onsite designee.

- Plan coordination.
    - This plan will be coordinated with appropriate physical security plans of adjacent facilities when possible. Mutual support agreements will also be established with companies having security interests in the local area.

4. *Security Inspections and Surveys*. Security inspections and surveys will be conducted routinely on a yearly basis. Non-routine risk assessments will be conducted whenever a significant loss occurs or other occurrence which may have a significant impact on the physical security of the facility.

5. *Security Risk Assessments are critical to security planning*. Risk assessments are used to adapt physical protective measures and security procedures to current conditions.

- Risk assessments must be performed on vulnerable areas. Risk assessments will be considered when scheduling follow-on inspections and surveys. Assessments will be kept on file until the next risk assessment is conducted.

6. *Restricted Areas*. One way we can safeguard assets is by declaring an area restricted and, thereby, limiting access to that area. Restricted areas will be designated and posted in accordance with local laws.

- This company will ensure all restricted areas have been assessed and local laws are complied with. Violations of restricted areas will be brought to the attention of the security officer and The Northeast Security Team or onsite designee .

7. *Security Measures*: There are two broad categories of security measures: procedural and physical. Measures instituted by this company should deter, detect, delay, or defeat the threat. Deterrence will be improved by using highly visible measures and randomness. This is cost-efficient and complicates the threatening person or group. Security measures will be integrated and layered by using a combination of lights, electronic security systems (ESS), and signs.

- Procedural controls will include but are not limited to: Security checks, checklists, written procedures, etc.

- Physical controls will include but are not limited to: Locks, lights, electronic security systems (ESS), and signs.

8. *General Access to Premises*:

   - Unrestricted areas. Any of the documents listed below may be used to gain access to facility. (Detail corporate policy)

   - Company & employee name must be listed on authorized vendor list

   - Photo ID (which is to be left with a Curaleaf employee)

9. *Policy for Passes and Badges*.

   - Issuing authorities within this company will keep a record of each access pass and badge issued or destroyed. Records will be maintained in a security binder.

   - Passes and badges are company property and may not be transferred or altered after they are issued. Lost passes or badges will be reported promptly to the issuing authority. When the need for a pass or badge ends, the individual's supervisor will ensure the pass or badge is voided and returned to the issuing authority. The issuing authority will destroy the pass or badge by cutting it into small pieces or shredding it and recording its final disposition. Supervisors will report passes and badges that cannot be recovered as "lost."

   - Lost or stolen passes will be reported to the individual's supervisor immediately.

   - The company may revoke passes with no prior notice.

   - To control and account for passes and badges, issuing authorities will:
     - Control procurement, storage, processing, issue, turn-in, recovery, expiration, and destruction of passes and badges.

     - Establish measures to reduce the possibility of theft, loss, counterfeiting, and improper use.

     - Arrange entry-control points so arriving and departing personnel must pass in single file in front of access-control personnel.

     - Authenticate security records as required.

     - Appoint a responsible custodian to perform control procedures.

     - Maintain written records that show the status of passes and badges, and the disposition of lost, stolen, and destroyed forms. Information will be recorded,

maintained, and destroyed according to company policy or on automated data files that include the same data elements.

- Promptly invalidate lost or stolen security badges and passes and maintain a current roster of invalidated badges and passes at access-control points.

- Maintain records at access-control points that enable access-control personnel to determine promptly and accurately the number and identity of persons in the area at any time.

- Permanent Badges. Permanent badges may be issued to a person requiring continual access to restricted areas. The permanent badge will have a clip-on attachment allowing it to be worn at all times on an outer garment while the bearer is in the restricted area.

- Temporary Badge. Temporary badges may be issued to visitors who require infrequent entry to a restrictive area or may also be used by personnel requiring continual access while a permanent badge is being prepared. Custodians may require visitors to release personal identification documents in exchange for a temporary badge or pass. When temporary badges are used, they will:

    - (1) Be laminated and have a clip allowing them to be worn on outer garment while in the restricted area.
    - (2) Be easily distinguishable from permanent security badges and passes. Visitors will be escorted at all times while in a restricted area. Entry and exit of visitors will be recorded.

10. *Access by Local Law Enforcement Agencies*.

- The Northeast Security Team or onsite designee and Facilities will:

    - Establish and conduct liaison with local law enforcement agencies.

    - Establish procedures for access by local law enforcement agencies.

    - Entry to Restricted Areas. Access to restricted areas will be provided for local law.

11. *Keys and Lock Controls (K&LC)*.

- Keys providing access to restricted areas that are not in use or are not attended will be stored in approved security containers or equivalent.

- Spare keys will not be kept with operational keys.

- Maintenance keys for high-security padlocks will not be used as primary access keys. Maintenance keys will be secured and will be kept separate from spare keys. Placing maintenance keys in a separate, sealed envelope in a container with the spare keys usually constitutes acceptable separation.

Research and Development Facility Security Procedures

- *Access to Facility*: Allow only registered qualifying patients, personal caregivers, Marijuana Research Facility agents, persons authorized by state regulations, and, subject to the requirements of state regulations, outside vendors, contractors, and visitors, access to the Marijuana Establishment.
- *No Loitering*: Prevent individuals from remaining on the premises following consultation.
- *Storage*: Store all marijuana products in a secure, locked safe and in such a manner as to prevent diversion, theft, and loss.
- *Locks*: Keep all safes, vaults, and any other equipment or areas used for the production, cultivation, harvesting, processing, or storage of marijuana and MIPs securely locked and protected from entry, except for the actual time required to remove or replace marijuana.
- *Lock Maintenance*: Keep all locks and security equipment in good working order.
- *Keys*: Prohibit keys, if applicable, from being left in the locks, or stored or placed in a location accessible to persons other than specifically authorized personnel.
- *Accessibility*: Prohibit accessibility of security measures, such as combination numbers, passwords, or electronic or biometric security systems, to persons other than specifically authorized personnel.
- *Perimeter Lighting*: Ensure that the outside perimeter of the Marijuana Establishment is sufficiently lit to facilitate surveillance.
- *Limited Access Area Signage*: All limited access areas must be identified by the posting of a sign that shall be a minimum of 12" X 12" and which states: "Do Not Enter – Limited Access Area – Access Limited to Authorized Personnel Only" in lettering no smaller than 1 inch in height.
- *Badges*: A Marijuana Research Facility Agent shall visibly display an identification badge issued by the state at all times while at the Marijuana Establishment or transporting marijuana.
- *Visitors*: All outside vendors, contractors, and visitors must obtain a visitor identification badge prior to entering a limited access area and shall be escorted at all times by an agent authorized to enter the limited access area. The visitor identification badge must be visibly displayed at all times while the visitor is in any limited access area. All visitors must be logged in and out, and that log shall be available for inspection by the Commission at all times. All visitor identification badges shall be returned to the Marijuana Establishment upon exit.

Registration of Agents

1. All board members, directors, employees, executives, managers, and volunteers who are associated with Curaleaf Processing Inc. must apply for Marijuana Research Facility Agent registration. All such individuals must:
    a. Be at least 21 years old; and
    b. Have not been convicted of an offense in the Commonwealth involving the distribution of controlled substances to minors, or a like violation of the laws of other jurisdictions; and

c. Be determined suitable for registration consistent with the provisions of 935 CMR 500.800: Background Check Suitability Standard for Licensure and Registration and 935 CMR 500.801: Suitability Standard for Licensure or 935 CMR 500.802: Suitability Standard for Registration as a Marijuana Research Facility Agent .

2. Information needed for registration of a Marijuana Research Facility Agent :
   a. The full name, date of birth, and address of the individual;
   b. All aliases used previously or currently in use by the individual including maiden name if any.
   c. A copy of the applicant's driver's license, government-issued identification card, liquor purchase identification card issued pursuant to M.G.L. c. 138, § 34B, or other verifiable identity document acceptable to the Commission.
   d. An attestation that the individual will not engage in the diversion of marijuana or marijuana products.
   e. Written acknowledgment by the individual of the limitations on their authorization to cultivate, harvest, prepare, package, possess, transport, and dispense marijuana for medical purposes in the Commonwealth
   f. Background information, including, as applicable:
      i. A description and the relevant dates of any criminal action under the laws of the Commonwealth, or an Other Jurisdiction, whether for a felony or misdemeanor and which resulted in conviction, or guilty plea, or plea of nolo contendere, or admission of sufficient facts;
      ii. A description and the relevant dates of any civil or administrative action under the laws of the Commonwealth, or an Other Jurisdiction, relating to any professional or occupational or fraudulent practices.
      iii. A description and relevant dates of any past or pending denial, suspension, or revocation of a license or registration, or the denial of a renewal of a license or registration, for any type of business or profession, by any federal, state, or local government, or any foreign jurisdiction.
      iv. A description and relevant dates of any past discipline by, or a pending disciplinary action or unresolved complaint by, the Commonwealth, or an Other Jurisdiction, with regard to any professional license or registration held by the applicant; and
   g. A nonrefundable application fee paid by the Marijuana Research Facility with which the Marijuana Research Facility will be associated.
   h. Any other information required by the Commission

3. Have the E.D. run a Criminal Offender Record Information (CORI) report for each individual for whom Curaleaf Processing Inc. seeks Marijuana Research Facility Agent registration, obtained within 30 calendar days prior to submission.

A. *Policies and procedures for maintaining confidential information in compliance with state regulations.*

Information held by Curaleaf Processing Inc. about registered qualifying patients, personal caregivers, and Marijuana Research Facility Agents is confidential and shall not be disclosed without the written consent of the individual to whom the information applies, or as required under law or pursuant to an order from a court of competent jurisdiction, provided however, the Commission may access this information to carry out official duties. Curaleaf Processing Inc.'s POS, patient registration, and order management systems (all within BT) are HIPPA compliant.

B. *Policies regarding security system maintenance and testing in compliance with state regulations.*

Surveillance Video:

- Twenty-four-hour recordings from all video cameras must be made available for immediate viewing by the Commission upon request
- Must be retained for at least 90 calendar days or the duration of a request to preserve the recordings for a specified period of time made by the Commission, whichever is longer.
- Motion detection sensor system will also be used by Curaleaf. This system will provide an alert to our The Northeast Security Team or onsite designee and Facilities. If an alert is sent or a sensor is not working correctly, we will take prompt action to make corrections and document the action made.
- Recordings must not be destroyed or altered, and must be retained as long as necessary if Curaleaf is aware of a pending criminal, civil, or administrative investigation, or legal proceeding for which the recording may contain relevant information
- Our video systems have the ability to immediately produce a clear, color still image whether live or recorded. A date and time stamp are embedded on all recordings which are synchronized and set correctly at all times. This time stamp does not obscure the picture in any way.
- All our systems are maintained by generator power can remain operational during a power outage for an unlimited amount of time.
- Within our system we can export a still image (in an industry standard format). Exported video has the ability to be archived in a proprietary format that ensures authentication of the video and guarantees the ability to be saved in a file that can be played on a standard computer operating system.
- All equipment is maintained in a secure, limited access location to prevent theft, loss, destruction, and alterations.
- Curaleaf obtains the services of two alarm companies. CGL is our primary which provides cameras, door access, and perimeter security. Instant Alarm or PSX will be our secondary service which provides motion detection.
- Access to surveillance areas shall be limited to persons that are essential to surveillance operations, law enforcement authorities, security system service personnel, and the Commission.
- A current list of authorized employees and service personnel that have access to the surveillance room must be available to the Commission upon request.
- Surveillance rooms must remain locked and must not be used for any other function.
- All security equipment must be in good working order; and

- Must be inspected and tested at regular intervals, not to exceed 30 calendar days from the previous inspection and test.

Security System Annual Audits

- Curaleaf Processing Inc. will, on an annual basis, obtain at its own expense a security system audit by a vendor approved by the Commission.
- A report of such audit will be submitted, in a form and manner determined by the Commission, no later than 30 calendar days after the audit is conducted.
- If the audit identifies concerns related to the Marijuana Research Facility's security system, the Marijuana Research Facility must also submit a plan to mitigate those concerns within 10 business days of submitting the audit.

C. *Policies and procedures as to how security systems will remain operable during a power outage in compliance with state regulations.*

In the event of a power outage, Curaleaf Processing Inc.'s security system is equipped with 24 hours of battery powered back-up supply to prevent any temporary lapses of coverage and each location will have a standby generator available. As soon as the power outage is identified a member of the EMT will contact the power company to understand exactly when the power outage occurred and when it will be resolved. In the event that all of the above fail or the power outage lasts more than 8 hours, Curaleaf Processing Inc. will report the incident to the CCC for further guidance and close the facility if required.

D. *Policies and procedures for transporting marijuana to laboratories for testing in compliance with state regulations.*

Prior to the distribution of marijuana or MIPs to the Lab, all products will be weighed and accounted for on video, their values and distribution will be entered into the electronic inventory management system. Individual shipping containers will be sealed with tamper evident tape, and a transport manifest will be securely transmitted via internet to the Lab. All manifests will be digitally retained in perpetuity.

Update: 01/19/2022

General Security Requirements for the marijuana Research Facility

- All waste containing finished marijuana shall be stored and secured in a locked container. *935 CMR 500.110(1) and 500.105(12)*
- No fewer than two (2) registered Marijuana Research Facility Agents will witness and document how waste is disposed. *935 CMR 500.110(1) and 500.105(12)*

- All finished marijuana shall be stored and secured in a locked container to prevent diversion or theft. *935 CMR 500.110(1)*
- All marijuana and marijuana products will be kept out of plain sight and will not be visible from a public place, outside of the Research Facility, without the use of binoculars, optical aids, or aircraft. All in-process work will be stored in a locked container at the end of the day. *935 CMR 500.110(1)*
- All entrances to the research and development facility will be secured via fob or key card to prevent unauthorized access. *935 CMR 500.110(1)*
- An emergency policy and procedure will be developed to secure all product following theloss of marijuana. *935 CMR 500.110(1)*

Limited Access Areas and Security and Alarms Requirements

- All limited access areas shall be clearly described by the filing of a diagram. *935 CMR500.110(4)*
- After a breach of security, the marijuana Research Facility will notify appropriate law enforcement authorities and the Commission in no more than 24 hours. *935 CMR 500.110(7)*
- The marijuana Research Facility will file an incident report following any breach of security within 10 calendar days. *935 CMR 500.110(7)*
    - All incident reports will be maintained for a period of one year or for the duration of an open investigation, whichever is longer. *935 CMR 500.110(7)*
- The marijuana Research Facility will have perimeter alarms. *935 CMR 500.110(5)*
- The marijuana Research Facility will have a failure notification system that provides an audible, text, or visual notification of any failure in the security system. The failure notification system shall provide an alert to designated employees of the marijuana Research Facility within five minutes after the failure, either by telephone, email, or text message. *935 CMR 500.110(5)*
- The establishment shall have video cameras in all areas that contain marijuana, at allpoints of entry and exit, and in the parking lot. *935 CMR 500.110(5)*
- The marijuana Research Facility will have video cameras directed at all safes, vaults, and areas in which marijuana is handled. Cameras shall be angled so as to allow for the capture of clear and certain identification of any person entering or exiting the marijuana Research Facility or area. *935 CMR 500.110(5)*
- All trees, bushes, and other foliage outside the establishment will be maintained to prevent persons from concealing themselves from sight. *935 CMR 500.110(5)*

Cash Handling Requirements

- Curaleaf Processing Inc. will not be handling cash at the Newton Research and Development Facility. The Research Facility will not be selling retail products.