

246 Commercial St.
PROPERTY ADDRESS OF PROJECT



19-22
CASE NO.

TOWN OF PROVINCETOWN PLANNING BOARD

SPECIAL PERMIT

TO THE TOWN CLERK, PROVINCETOWN, MASSACHUSETTS: (please print legibly)

1. The undersigned hereby files with specific grounds for this Special Permit application:
Applicant seeks a **Special Permit** under:

- Article 2, Section 2440, Permitted Principal Use, Accessory Dwelling Units (under footnote 20 & 21 Use table)
- Article 2, Section 2440, Permitted Principal Uses, B13, Large Scale Ground-Mounted Solar;
- Article 2, Section 2440, Permitted Principal Uses, B14, Marijuana Establishment, Retail;
- Article 2, Section 2440, Permitted Principal Uses, B15, Marijuana Establishment, Industrial;
- Article 4, Section 4180, Inclusionary and Incentive Zoning Bylaw, Development of two or more dwelling units; or
- Article 7, Section 7080, Application Requirements, Wireless Telecommunications Towers & Facilities.

2. **PRIOR RELIEF GRANTED TO PROPERTY:** SPECIAL PERMIT VARIANCE UNKNOWN

3. **PLEASE ATTACH A NARRATIVE DESCRIBING YOUR PROJECT**

4. Applicant/Representative Ezra Parzybok ezra@greenglove.cc
 (full name) (email)
 139 Damon Rd. #5 Northampton, MA 01060 413-539-3059
 (mailing address including zip code) (phone number)

5. Owner (if other than applicant) Andrew Koudijs akoudijs@hennep.com
 (full name) (email)
 200 Brookline Ave Apt. 3 Boston, MA 02215 914-483-9167
 (legal mailing address including zip code) (phone number)

6. Property located at: 246 Commercial St. (email) Assessors Map & Parcel Map 11-3, 50 Zoning District commercial
 Present use of premises Retail Proposed use of premises Cannabis Retail

7. Deed Book & Page: Bk 25598 Pg. 12 or Land Court Certificate #: _____

Signing this application declares that the statements and information on the foregoing application are true and accurate, to the best of your knowledge and belief. Signing this application also signifies that you have read and fully understand the attached instructions and general information

Applicant's Signature [Signature]
 Owner's Signature [Signature]

11/10/18
 date
 11/10/18
 date





246 Commercial St. Provincetown
Special Permit Narrative

Special Permit Narrative for Hennep, Inc. a proposed retail cannabis establishment

Table of Contents:

<u>Narrative</u>	<u>p.3</u>
<u>Security</u>	<u>p.3</u>
<u>Generator</u>	<u>p.4</u>
<u>Renovation</u>	<u>p.5</u>
<u>Transportation</u>	<u>p.5</u>
<u>Pedestrian Foot Traffic</u>	<u>p.5</u>
<u>Parking</u>	<u>p.5</u>
<u>Deliveries</u>	<u>p.6</u>
<u>Exterior and Landscaping</u>	<u>p.6</u>
<u>Developmental Impact Statement</u>	<u>p.6</u>
<u>Community Impact</u>	<u>p.7</u>

Narrative:

Hennep, Inc. (Hennep) is a proposed cannabis retail establishment owned by Andrew Koudijs of Boston, MA. Hennep proposes to be a state licensed, fully compliant, retail marijuana establishment located at 246 Commercial Street. Hennep will share the existing building currently containing two retail sites (the other retailer is the Provincetown Bookshop.) The proposed commercial space is approximately 500 square feet and the building is owned by Joel Newman RLT who will provide the lease. Hennep will adhere to all Cannabis Control Commission (CCC) regulations and all Provincetown permitting and licensing requirements and recommendations for operations, entrance and perimeter security, fire safety, secure product storage, prevention of diversion, lab testing of all products, employee handling of product, waste disposal, and community engagement.

Hennep intends to provide the adult-use market in Provincetown with consistent, lab-tested cannabis products, and has signed a host agreement with the town. No persons under 21 years of age will be able to enter the building and as public consumption is prohibited throughout the state, cannabis products will be sealed in tamper and child-resistant packaging, allowing the consumer to safely access products in his or her private residences. Hennep will follow all Fire regulations put forth in 527 CMR and with Chapter 38 of the NFPA 1 (2018).

Security:

Hennep, Inc. has contracted with American Alarm, a professional security and alarm service provider to design, implement and execute a comprehensive security system – to be approved by the chief of police – that will ensure that the retail store is a safe and secure environment for employees and the local community, without compromising Commercial Street charm. The security system will consist, among other things, of perimeter cameras on all exit and entry

points, as well as duress, panic, or hold-up alarms as specified or recommended by the security consultant for efficient notification and response in the event of a security threat.

The system will also include a back-up security platform as required in the state regulations as well as an on-site generator or battery, allowing the alarm system and surveillance cameras to remain operational in the event of a power outage.

An on-site licensed marijuana agent who checks ID's will be stationed at the entry during all hours of operation.

In addressing the perceived cash and carry challenge of many dispensaries, Hennep plans to allow customers to use debit cards, reducing the need for cash. Massachusetts now has banks serving the marijuana industry and we will utilize this banking system.

Hennep has included two copies of a complete Retail Security Plan in the special permit application as well.

Generator:

Hennep, Inc. has consulted with David Oles of American Alarm Systems who has designed over 20 dispensary security systems in the state. It is intended that the alarm system will be equipped with an independent, Uninterrupted Power Supply (UPS) that will automatically provide continual power in the event of a power failure or interference with the regular power supply. The security cameras will be supported by a back-up power generator that will, again, sustain their operation in the event of a power failure or interference with the regular power supply. Generator technology has advanced greatly in recent years. Current state-of-the-art generators suitable for our intended application produce a "low hum" when activated, and will not disturb abutters with noise during a power outage. Its proposed location is in the private back yard on the side of the building and will be powered by an adjacent propane tank.

A *Tesla Power Wall* battery (or competitor such as Honda, LG Chem, Mercedes, etc.) can also be utilized as a tertiary back-up option, which will supply power for several days in the event of an outage or generator failure.

Renovation Plans:

Retaining as much of the inherent charm of the “art deco” inspired building, Hennep, Inc. intends to make no external changes to the structure other than a Hennep sign outside the building and cosmetic improvements such as paint. The interior fit-out will open up a currently unused storage area to allow a longer queue line to extend into retail space. Stock and valuables will be safeguarded within a purpose-built security vault equipped with secure, touch pad access. The installation of this vault will require no changes to exterior walls.

Transportation Impact:

The decision to select this location was primarily driven by its pedestrian accessibility. The shop at 246 Commercial is ideal for numerous reasons. Chiefly, it blends well with the style and tone of the retail district as a whole and avoids the “corporate” look of many dispensaries currently being created in the first wave of legalization. These, we feel, can easily detract from a seamless pedestrian shopping experience: And importantly, the space’s floor plan provides almost 50 linear feet inside the building to accommodate an off-street, interior queue.

Pedestrian Foot Traffic:

With a full special permit review, Hennep, Inc. will comply with the maximum occupancy determined by the town, but could potentially provide space for a sufficient internal queue which would prevent the need for any line outside the building during business hours. Hennep intends to also maximize the technology readily available at popular restaurants, cannabis dispensaries, and other destinations that mitigate lines. These can include text message when a registered client’s order or place in line is available as well as incentives for visiting the store during off times.

Parking:

Parking for Hennep, Inc. is conveniently located nearby at the Ryder Street Lot, the Grace Hall Parking Lot, and McMillan Pier Parking Lot. Due to the ample parking in these lots, we anticipate that Hennep will be a pedestrian destination. We envisage that any increased pedestrian activity that Hennep creates will also be of benefit to other retailers in the community as it is a year-round business. Hennep will have an active website which will encourage clientele to walk from the ferry or park in the nearby lots. No vehicles other than deliveries will be allowed to park or idle outside the store.

Deliveries:

Hennep anticipates a weekly delivery which will occur before or after business hours and during a time of least pedestrian traffic flow. We will notify the police department of our delivery schedule if necessary. As the state requires two agents in every delivery vehicle, one agent can be available to move the vehicle if necessary and the other agent will unload, a scenario similar to other shops on the street that only have automobile access in front. The cannabis products will come in individually locked boxes that can only be opened by licensed marijuana agents.

Exterior and Landscaping:

We do not anticipate any alteration to landscape, architecture, or the site around the establishment and plan to address minor cosmetic issues such as painting and window coverings only. Exterior signage for Hennep will follow local regulations and CMR 500.105 (4) (a) which states that *“use of medical symbols, images of marijuana, related paraphernalia, and colloquial references to cannabis and marijuana are prohibited from use in this logo.”*

Development Impact Statement:

The pedestrian nature or our anticipated customer flow in and around our proposed retail location is in keeping with the other stores in the area. Due to the state-required Host Agreement, Provincetown will receive up to 3% of total gross sales, and a further 3% of gross sales as a local sales tax. We feel that as the only industry that is required to provide the town with such funds, these funds will more than cover the additional administrative costs that town

might incur via inspections, accounting, etc. and thus the impact to the community will be a net gain. In our discussion with community members at the Community Outreach Meeting, cannabis is enjoyed by a large percentage of summer, off-season and permanent residents and tourists. We feel that providing a safe, legal, and comfortable space to procure this product will contribute further to this net gain; it will not bring a product or service that will disrupt or discourage the Provincetown culture and economy.

Community Impact:

Although adult-use marijuana has been recently legalized in Massachusetts, its presence in the state is not new. Medical marijuana has been legal since 2012, with little evidence of negative impact to communities and currently any adult 21 years or older can legally grow marijuana at home. Due to the lack of evidence detailing health harms of marijuana beyond those of over the counter drugs, alcohol, or cigarettes, we feel the negative impact marijuana has had on communities is primarily a policing and criminal justice issue- a burden both for the law enforcement side as well as consumer side. Hennep believes that providing a safe, legal, and adult-oriented retail establishment in an accessible and safe area of the downtown shopping district will create a net benefit in this policing and criminal justice issue as well as bring pedestrians and shoppers who are seeking a legal source of cannabis.

A March 2018 article in Forbes magazine which quoted a report on legal marijuana’s community impact states that, “the report is notable in dispelling some of the harms that are often attributed to legalization: The researchers found no evidence that legal cannabis contributed to increased homelessness or increased youth use of marijuana.”¹

Hennep also intends to provide numerous measures in order to mitigate the potential diversion to minors, as well as to provide education and service in the community. Hennep will train and incentivize employees to scrutinize identification to verify that consumers are 21 years and

¹ <https://www.forbes.com/sites/monazhang/2018/03/13/legal-marijuana-is-a-boon-to-the-economy-finds-study/#39ca9ea4ee9d>

older. Any ID found to be illegitimate or any evidence discovered that points to diversion of marijuana will result in a financial bonus to the employee. Any employee found to have engaged in diversion will be terminated.

As the scientific and anecdotal evidence comes out revealing the analgesic,² anti-emetic,³ and anti-anxiety⁴ benefits, etc. of marijuana many older citizens are seeking relief from non-toxic cannabinoids produced by the plant. According to a National Institute of Health study, the fastest growing demographic who consumes cannabis are citizens over 50 years old. The study reports a 57.8% relative increase [in cannabis use] for adults aged 50–64. These findings help dispel the assumption that a retail marijuana establishment would primarily attract and serve a younger demographic.

In dispelling the perception that marijuana might lead to harder drug use, a Journal of Pharmacology study found that, "Among respondents that regularly used opioids, over three-quarters (76.7%) indicated that they reduced their use since they started medical cannabis. This was significantly ($p < 0.0001$) greater than the patients that reduced their use of antidepressants (37.6%) or alcohol (42.0%). Approximately two-thirds of patients decreased their use of anti-anxiety (71.8%), migraine (66.7%), and sleep (65.2%) medications following medical cannabis."⁵

In clinical settings, marijuana use is also associated with reduced cravings for cocaine and opiates. According to the *Addictive Behaviors* study, "...we observed that a period of self-

² Russo, Ethan B. "Cannabinoids in the Management of Difficult to Treat Pain." *Therapeutics and Clinical Risk Management* 4.1 (2008): 245–259. Print.

³ Br J Pharmacol. 2011 Aug;163(7):1411-22. doi: 10.1111/j.1476-5381.2010.01176.x. Regulation of nausea and vomiting by cannabinoids.

⁴ Tambaro, Simone, and Marco Bortolato. "Cannabinoid-Related Agents in the Treatment of Anxiety Disorders: Current Knowledge and Future Perspectives." *Recent patents on CNS drug discovery* 7.1 (2012): 25–40. Print.

⁵ Substitution of medical cannabis for pharmaceutical agents for pain, anxiety, and sleep, Journal of Psychopharmacology, 2017 <https://www.ncbi.nlm.nih.gov/pubmed/28372506>

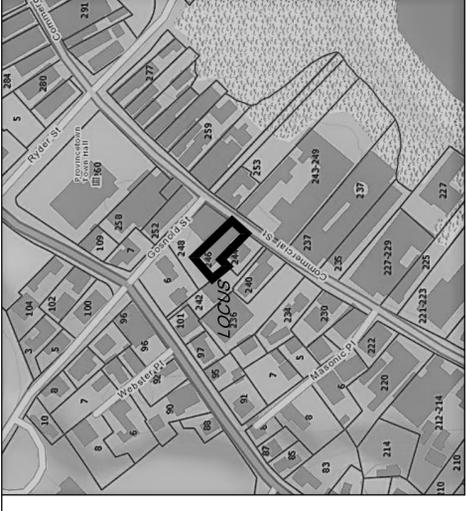
reported intentional use of cannabis ... was associated with subsequent periods of reduced use of crack [cocaine]. ... Given the substantial global burden of morbidity and mortality attributable to crack cocaine use disorders alongside a lack of effective pharmacotherapies, we echo calls for rigorous experimental research on cannabinoids as a potential treatment for crack cocaine use disorders."⁶

Evidence supporting the correlation between legal marijuana dispensaries and the reduction of opiate use, dependence, and overdoses in communities is also detailed in a report by the National Institute of Drug Abuse.⁷ It is an assumption that medical marijuana products differ from adult-use products, but as there has been criticism in the state about the lack of education in Registered Medical Marijuana Dispensaries, Hennep intends to provide quality, tested marijuana products that will support both medical marijuana patients as well as adult-use consumers.

The team at Hennep feel that our retail establishment will provide a positive and net benefit to the town, will not disrupt vehicular or foot traffic more so than other shops on Commercial Street, will maintain the culture and architecture of the shopping district, will have state of the art security, and will provide the maximum 3% of gross sales, 3% of tax revenue, as well as the additional benefits to the town outlined in the host agreement.

⁶ Intentional cannabis use to reduce crack cocaine in a Canadian setting: A longitudinal analysis, *Addictive Behaviors*, 2017

⁷ <https://www.drugabuse.gov/news-events/nida-notes/2016/05/study-links-medical-marijuana-dispensaries-to-reduced-mortality-opioid-overdose>



Gosnold Street

Proposed Electrical Generator
on a 3' x 6' Concrete Pad

#248-250 Commercial Street
Vin's Emma LLC
Deed Book 16682, Page 215
Plan Book 362, Page 42
"Multi-Use Residential" per the Assessors Office

N 49°03'58" E 48.69'

S 44°22'18" E 90.00'

#246 Commercial Street
2-Residential Apartments (Upper Floors)
2-Retail Businesses (Ground Floor)

#242 Commercial Street
Timothy F. Barry
Deed Book 10022, Page 104
Plan Book 336, Page 26
"Small Retail" per Assessors Office

N 40°58'30" W 34.00'

S 43°20'16" W 17.00'

#244 Commercial Street
Commercial Point LLC
Deed Book 30776, Page 131
Plan Book 331, Page 39
"Small Retail" per the Assessors Office

Commercial Street,
22' Undefined Public Way
S 36°43'25" W 34.26'

- Legend
- Bicycle Rack
 - Heat Pump
 - Propane Tank
 - Water Valve



Site Plan of Land
#246 Commercial Street,
Provincetown, MA
prepared for
Andrew Koudijs
Scale 1" = 10' Nov, 12, 2018
Ols#758001



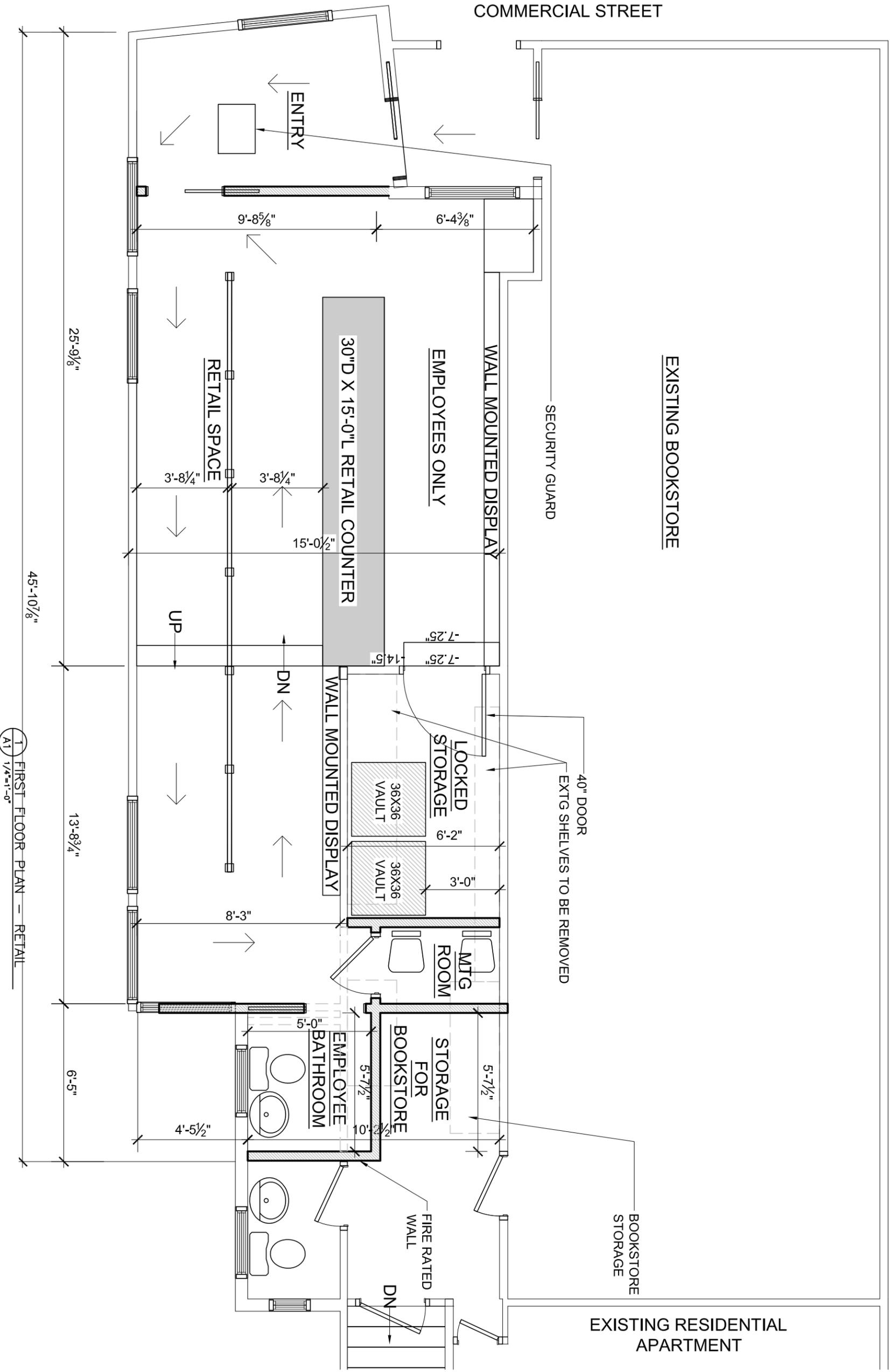
I hereby certify that the structures shown hereon
are located as they exist on the ground.

Donald T. Poole PLS #32662 Date

Zoning District = TCC Town Center Commercial
Minimum Lot Area = 5,000 Sq.Ft. (Existing Lot = 3,681 Sq.Ft.)
Minimum Lot Frontage = 50' (Existing Lot = 34.26')

Lot Area = 3,681 Sq. Ft.
Building Area = 2,157 Sq. Ft. or 58.6% of Lot.
Concrete, Brick, and Gravel Walks = 826 Sq.Ft. or 22.4 % of Lot.
Green Space = 696 Sq. Ft. or 19% of Lot, Existing / 678 Sq.Ft. or 18.4% Proposed

AREA CALCULATIONS:
PROPOSED CONDITIONED SPACE:
 BOOKSTORE: ± 860 SF
 RETAIL SPACE: ± 650 SF
 APARTMENT: ± 590 SF



1 FIRST FLOOR PLAN - RETAIL
 A1 1/4"=1'-0"

A RENOVATION FOR:
 HENNEP
 246 COMMERCIAL STREET
 PROVINCETOWN, MA

TITLE:
 PLANS

831 Main Street
 Dennis, MA 02638
 508.694.7887 phone
 www.a3architectsinc.com

A3 architects, inc
 Residential Commercial Net Zero

Date: 06.07.2018
 EXTG: 10.29.2018
 REV: 10.29.2018

A-1

NOTICE OF COPYRIGHT:
 THIS DRAWING IS THE PROPERTY OF THE ARCHITECT HAS BEEN PREPARED SPECIFICALLY FOR THE OWNER FOR THIS PROJECT AT THIS SITE AND IS NOT TO BE USED WITHOUT WRITTEN CONSENT OF THE ARCHITECT
 © A3 ARCHITECTS, INC. 2018

Hennep, Inc
RETAIL STORE
SECURITY PLAN

Introduction

Roles and Responsibilities of the Security Manager

Security Systems

- Alarms
- Video Surveillance
- Recording Standards

Access Control

- Retail Facility
- Sales Floor
- Key/Card Procedures
- Access Levels
- Lost/Stolen Card/Key Procedures
- Locks Cabinets and Safes
 - Keys
 - Codes
 - Combinations
 - Changes to Codes and Combinations

Product Diversion

- Diversion through Sales
- Diversion through Theft

Store Opening Procedures

Store Closing Procedures

Waste Disposal

- Regular Waste Disposal
- Marijuana Waste Disposal

Storage, Inventory Control, and Reconciliation

Shipping and Transportation Security

Incident Reporting

Security Procedures and Emergency Responses

- Armed Robbery Procedures
- After the Robbery
- Inventory theft
- Fire in Facility

Information Technology Security

- Acknowledgement
- Employee Administration

- Contractors and Temporary Workers
- Acceptable Use
- Equipment and Media Security
- Security Controls
- Security Logging and Monitoring
- Third-Party Access
- Access Control
- System and User Accounts
- Passwords
- Account Review
- Network Connectivity
- Changes to Applications
- Security Incident Response/Disaster Recovery
- Compliance and Audit

Introduction

Hennep, Inc will meet all security requirements in accordance with Massachusetts state law and Cannabis Control Commission regulations, as well as any local security requirements mandated by the town of Provincetown. This security plan should be shared appropriately with local law enforcement authorities and fire services, as should any material change or revision of this plan.

Security Audits

In accordance with 935 CMR 500.110 (8) conduct an annual security system audit by a vendor approved by the Commission. A report of such audit must 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 facility's security system, the company must also submit a plan to mitigate those concerns within ten business days of submitting the audit.

Roles and Responsibilities of the Security Manager

The Retail Store Manager is also the primary Security Manager for our facility. In the absence of the Retail Store Manager their Security Management responsibilities will be assumed by their deputy - generally, the Assistant Retail Store Manager. In any event, the assigned Security Manager must be trained and tested in the needs, requirements, and responsibilities of this essential role. The key responsibilities of the Security Manager role are:

- The safety of customers, staff, and visitors to the facility.
- The training of staff in all security-related procedures
- The prevention of diversion
- The safe and secure storage of inventory
- The integrity of perimeter and facility security
- Ensuring that all security systems and technologies function correctly, meet legal and code requirements, and are regularly maintained to prevent failure and ensure compliance.
- The enforcement of all security-related matters.

Security Systems

All security systems will be maintained in good working order and will be inspected and tested at regular intervals, not to exceed 30 calendar days from the previous inspection and test.

Alarms

- The primary facility alarm system will be centrally monitored by a licensed alarm company who are also properly licensed for both installation and maintenance. The facility will have both internal and external closed-circuit camera monitoring, as well as security lighting, perimeter entry point alarms, motion detectors, pressure switches, etc.
- In addition, a secondary, back-up alarm system monitored by a separate, licensed alarm company who are licensed for both installation and maintenance will be installed.
- The master code to either turn off or bypass the alarms will only be known to managers and/or keyholders, and should be changed whenever someone trusted with it leaves the company, or on a quarterly basis to insure it does not get stale and misused.
- Control panels for the alarm systems will be located in a closed cabinet by the main entrance to the retail store.
- The alarm systems will also include the following functionality:
 - Battery back-up for the system in the event of power outage.
 - A failure notification system that provides an audible, text, or visual notification of any failure in the surveillance system. The failure notification system will provide an alert to designated employees of the retail facility within five minutes of the failure either by telephone, e-mail, or text message.
 - Silent mode to protect employees if perpetrators are armed.
 - Duress and Panic alarms
 - Visual alert (flashing lights on the exterior of the building to notify passing police a robbery is in progress).
 - Cell phone back-up in event telephone or internet connection is cut.
- Areas covered by the alarm system will primarily be those places that are the usual points of entry for most facilities. These include doors, skylights, windows, interior doors and windows, and parts of the interior that require high security because of valuable inventory and or risk areas for employees.
- The sensor types for the alarm system will include magnetic door contacts, glass break sensors, trap alarms, vibration sensors, fire sensors, motion sensors, duress or panic alarms, and also both wireless and hard-wired sensors.
- The physical design and placement of alarm components is a critical part of the system. Our security design team will, apart from the above, focus on motion-sensitive illumination, reinforced doors and windows. and ensuring that the entire counter area is viewable by other store employees. A height reference tape will be placed near the entrance and, where practicable, by the counter.

Video Surveillance

- The surveillance system will be monitored and functional 24 hours a day. The system will monitor both the interior and exterior of the facility, and will be an IP (Internet Protocol) based technology that will allow management, and, if necessary, law enforcement and other regulators the ability to observe the camera system securely through a web-based browser, either on a computer system or a smartphone.

- The server, control system, telecommunications system, and back-up power supply for the video and recording system will be permanently installed in a suitably reinforced “surveillance room” that will not be used for any other purpose. Access to this room will be strictly limited to employees that are essential to security, 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.
- Critical areas- internal - including all limited access areas, vaults, safes, points of sale, points of ingress/egress and all active and inactive point of sale areas ensuring that the entire counter area is viewable by the video surveillance system. A height reference tape will be placed near the entrance and, where practicable, by the counter.
- Critical areas - external - including the full perimeter of the facility, all entrances, the parking lot, and parking lot entrance.
- Trees bushes and other vegetation will be regularly trimmed and maintained to ensure full visibility and deny opportunities for concealment.
- The system will be a complete video system, i.e., it will not only monitor the facilities, it will record all activities and archive them for the statutory period of time. Camera resolution will be HD 1080 to provide satisfactory detail and be angled to allow for the capture of clear and certain identification of any person entering or exiting the retail facility or area.
- The security company charged with the installation of our security system is bonded, licensed and insured. The facility video system will be installed by a licensed security company who are properly licensed for both installation and maintenance
- All video recordings from all cameras must, upon request, be made available for immediate viewing by the Commission.
- All video recordings must be retained for at least 90 calendar days.
- No video recording may be destroyed or altered, and shall be retained as long as necessary if the company is aware of a pending criminal, civil or administrative investigation or legal proceeding for which the recording may contain relevant information.

Recording Standards

- All video recordings will have a date and time stamp embedded in the recordings, which will be synchronized and set correctly at all times and shall not significantly obscure the image.
- The system will have the capability of immediately producing a clear, color, still photo whether live, or recorded. In accordance with 935 CMR 500.110 (5) such images will be in an industry standard format including .jpg, .bmp and .gif. Exported video will have the ability to be archived in a proprietary format that ensures authentication of the video and guarantees that no alteration of the recorded image has taken place. Such exported video will also have the ability to be saved in an industry standard file format that may be played on a standard computer operating system.
- All recordings must be erased or destroyed prior to disposal.
- The video and recording system will be equipped with a battery back-up for the system in the event of power outage.

Access control

Retail Facility

- When closed for business the facility will be closed and secured in accordance with the closing procedures outlined below.
- When opening for business the facility will be opened in accordance with the opening procedures outlined below.
- All employees of the facility will visibly display an employee identification badge issued by the company at all times while at the retail facility.
- All outside vendors, contractors and visitors shall be provided with a visitor identification badge prior to entering a limited access area, and shall be escorted at all times by a company licensed marijuana agent. The visitor identification badge will be worn visible at all times. All visitors must be logged in and out and that log shall be available for inspection by the Commission at all times.
- In accordance with 935 CMR 500.110 (1) (e) and 935 CMR 500.110 (4), all employees will be issued with an electronic “swipe” card that affords them access to certain rooms and spaces within the facility. .
- These cards track the time and individual gaining access to the various restricted areas.
- The functionality of these “swipe” cards will vary depending on the requirements of the roles of individual employees. The access granted by such cards is laid out, in general terms, in the “Access levels” section below.
- **No swipe card or keys will be issued to any person that is not a state licensed marijuana agent.**
- Certain managers will be designated as keyholders. These individuals may be provided with keys, codes and combinations that afford them access to the building, vault, and other restricted areas. In accordance with 935 CMR 500.110 (1) all keys held by keyholders will be secured to their clothing or person with a key-chain or lanyard at all times.
- **No key, code, or combination will be issued to any person that is not a state license marijuana agent and employee of the company.**
- In accordance with 935 CMR 500.105 (14) the following individuals shall have access to a marijuana establishment or marijuana establishment transportation vehicle:
 - Representatives of the Commission in the course of responsibilities authorized by St. 2016, c. 334, as amended by St. 2017, c. 55 or 935 CMR 500.000
 - Representatives of other state agencies of the Commonwealth; and
 - Emergency responders in the course of responding to an emergency
- 935 CMR 500.000 shall not be construed to prohibit access to authorized law enforcement personnel or local public health, inspectional services, or other permit-granting agents acting within their lawful jurisdiction.
- In accordance with 935 CMR 500.110 (4) all limited access areas will be identified by the posting of a sign at least 12” by 12” stating: **“Do Not Enter - Limited Access Area - Access Limited to Authorized Personnel Only”** in lettering no smaller than one inch in height.
- Limited access areas shall be clearly described by the filing of a diagram of the registered premises, in the form and manner determined by the Commission.

Sales Floor

- In accordance with 935 CMR 500.110 (1) (a) and 935 CMR 500.105 (14), **NO** person may enter our retail premises without first producing a valid, state or federal, photo ID.
- Valid ID must be presented to the responsible member of staff at the entrance to the retail store

and at the Point of Sale for data-entry purposes.

- No person under 21 years of age may enter the premises. There are **NO** exceptions to this rule.
- While a person of legal age is welcome to accompany a customer into the store, loitering, in accordance with 935 CMR 500.110 (1) (b) is not permitted under any circumstances.
- Any person suspected of loitering should be politely questioned by a member of staff and, if unable to credibly account for their presence, be asked to wait outside the facility. Should the person refuse, the matter should be elevated to the store manager who may, if necessary, contact local law enforcement for assistance in removing the person from the facility.

Key/Card procedures

Entry to restricted areas with a “swipe” card can only be made by authorized personnel. It is **NOT** permissible to provide access to another employee to any area using your personal card.

Allowing or providing access to unauthorized persons is grounds for immediate dismissal.

Access levels

- **Managers** - Store managers will have access to ALL areas and, furthermore, will be responsible for the issue, management, and cancellation of all “swipe” cards, and the sign-out and management of all internal-use keys to safes, cupboards, and storage areas. Senior management will be responsible for the issue of keys for building entry, and the management and issue of all codes and combinations. Assistant managers and managers, as keyholders may be provided with keys for building entry depending upon their role, responsibilities, and the requirements placed upon them at the discretion of senior management.
- **Employees** - Will be provided with a “swipe” card that provides them access to the rooms and spaces necessary for the fulfilment of their role and responsibilities.
- **Owners and Investors** - Will **NOT** be provided with any key, “swipe” card, code or combination unless they are a licensed marijuana agent with a role that requires access. Entry to the facility by such persons may only be facilitated by the store manager or senior management under the same terms as any other visitor (see Visitors, below).
- **Visitors** - Must wear a “Visitor” badge at all times when in the facility. A “Visitor” badge will be issued once the individual’s details have been entered in the log book provided. All visitors are to be accompanied by a licensed marijuana employee at ALL times.
- **Contractors**
Must wear a “Visitor” badge at all times when in the facility. A “Visitor” badge will be issued once the individual’s details have been entered in the log book provided. All contractors are to be accompanied by a licensed marijuana employee at ALL times.

Lost/Stolen card/key procedures

Each card has an individual serial number that is assigned to the authorized employee. In the event that a “swipe” card is lost or stolen the following steps must be taken:

- The store manager must be notified in person **IMMEDIATELY** the loss is identified.
- It is **NOT** acceptable to leave a message on an answering service, send a text or e-mail, or leave a message with another person or through other means. **THE STORE MANAGER MUST BE NOTIFIED IN PERSON.**
- In the event the store manager cannot be reached the current or subsequent or duty manager must be informed on the same terms as above.
- The holder of the lost card should notify the manager when, where, and how they believe the card was lost.

- The store manager (or duty manager) must immediately access the system and cancel the “swipe” card in question.
- The employee must complete a “Security Device Loss” form that documents when, where, and how they believe the card was lost. In the event that the employee believes the card was stolen, a police report **MUST** be filed with local law enforcement and the Commission informed.
- A new card may only be issued upon completion of the above steps.
- Loss of a replacement card may be grounds for dismissal.

Building access keys are issued to responsible managers. In the event that a building access key is lost or stolen the following steps must be taken:

- A senior manager must be notified in person **IMMEDIATELY** the loss is identified.
- It is **NOT** acceptable to leave a message on an answering service, send a text or e-mail, or leave a message with another person or through other means. **THE SENIOR MANAGER MUST BE NOTIFIED IN PERSON.**
- In the event the senior manager cannot be reached, the store manager must be informed on the same terms as above.
- The holder of the lost card should notify the senior manager when, where, and how they believe the card was lost.
- The senior manager or store manager must immediately attend the store with their personal set of building access keys.
- A locksmith will be called and all compromised locks will be changed immediately.
- The manager or individual responsible for the loss must complete a “Security Device Loss” form that documents when, where, and how they believe the keys were lost. In the event that the individual believes the keys were stolen, a police report **MUST** be filed with local law enforcement and the Commission informed.
- The senior manager will supervise the recall and replacement of all building access keys.

Secure storage keys are issued to responsible managers and keyholders. These keys may not be handed to any unauthorized person or employee. In the event that a secure storage key is lost or stolen the following steps must be taken:

- The duty store manager must be notified in person **IMMEDIATELY** the loss is identified.
- The custodian of the lost key(s) should notify the duty store manager when, where, and how they believe the key(s) was lost.
- The store manager will immediately lock the secure storage area using the reserve key kept in the safe.
- A locksmith will be called and all compromised locks will be changed immediately.
- The manager or individual responsible for the loss must complete a “Security Device Loss” form that documents when, where, and how they believe the keys were lost. In the event that the individual believes the keys were stolen, a police report **MUST** be filed with local law enforcement and the Commission informed.
- A senior manager will supervise the recall and replacement of all secure storage keys.

Locks, Cabinets, and Safe protocols

Internal security practices require that certain drawers, cabinets, cash boxes, safes and vaults are secured with either a key lock, code lock, or combination lock. In the course of normal business it may be necessary for employees to access these secure areas. The following outlines the protocols, procedures and practices associated with the security devices.

Keys - Secure storage keys are issued to responsible managers. These keys may not be handed to any unauthorized person or employee.

- It is the responsibility of the store manager or keyholder to open the secure storage device or area, witness the tasks performed and ensure ensure that the secure device or area is secured once more following the completion of the task for which access was required.

Codes - Certain secure devices and areas are equipped with a keypad or code to deny access to unauthorized persons.

- Under no circumstances may such codes be shared with unauthorized personnel. It is the responsibility of the store manager or keyholder to enter these codes on behalf of employees wishing to gain necessary access.
- It is the responsibility of the same store manager or keyholder to ensure that the secure device or area is secured once more following the completion of the task for which access was required.
- Codes may not be written down, noted, recorded, texted, or e-mailed to any individual at any time.

Combinations - Certain secure devices and areas are equipped with a combination lock to deny access to unauthorized persons.

- Under no circumstances may such combinations be shared with unauthorized persons. It is the responsibility of the store manager or keyholder to enter these combinations on behalf of employees wishing to gain necessary access.
- It is the responsibility of the same store manager or keyholder to ensure that the secure device or area is secured once more following the completion of the task for which access was required.
- Combinations may not be written down, noted, recorded, texted, or e-mailed to any individual at any time.

Changes to codes and combinations - From time to time, and in the interest of best security practices, codes and combinations will be changed.

- Senior Management will be responsible for the scheduling and change of such codes and combinations
- All changes to codes and combinations will be provided to authorized recipients **IN PERSON**.
- Codes and combinations may not be written down, noted, recorded, texted, transmitted or e-mailed to any individual at any time.
- Upon receiving any new code or combination the **event** will be recorded in the “Security Device Log” and signed by both the provider and recipient of the new code or combination.

Store Opening Security Procedures

The keyholder or manager on duty is responsible for unlocking the store, opening the gates, turning off the alarm, checking beginning inventory, and preparing for opening.

The general order of opening, from a security perspective, is as follows:

- Manager or keyholder and one other member of staff should arrive 30 minutes prior to store opening to insure readiness.
- Under no circumstances should the manager or keyholder open or enter the facility alone.
- The perimeter and outside of the facility should first be inspected visually. If there is evidence of any tampering with the lock, or attempted break-in, the manager must call the police and not enter the facility.
- Unlock and enter the building. Insure that no error or activation codes are present on the alarm system.

If the alarm system indicates that an alarm has been activated, leave the building, lock the doors, contact the alarm company and local law enforcement and await their attendance. Otherwise:

- deactivate the alarm and relock the point of entry from within. The manager must know and be trained in using the "duress code" in the event he or she is ambushed at opening.
- Turn on lights for store operations.
- Perform a visual check to insure all windows, inventory, and physical assets are undisturbed.
- Open the vault and place sales stock carts in sales area.
- Open the safe, and place cash drawers in respective registers.
- Exit and lock the vault
- Insure security cameras are operational and recording from monitor in back office.
- Call security company and perform daily check of "panic" buttons.
- Insure that front door and exit doors are locked and only opened to admit other employees as they arrive.

Store Closing Procedures

In accordance with 935 CMR 500.110 (1) (d), the facility must be secured to prevent and deter unauthorized access. Before you leave at night, always ensure that all cash and sales stock are placed in the vault and secured. The end of the evening shift should be used to ensure that sales inventory is audited, cash is counted, and that all employees exit safely.

- Do not extinguish or dim any lights until all customers have left the facility.
- Do not close the registers until after the scheduled closing, and ensure all customers have exited the store. Check all offices and restrooms to ensure there is no one left but employees.
- Check the phone for any unanswered voicemail.
- Empty all trash receptacles, and place trash bags at rear of store. Any trash that must be taken out must be checked by the manager to ensure no product is being covertly removed.
- Place trash bags at door for removal and disposal upon exit.
- Look outside and ensure that the parking lot and store exit safety lights are on.
- When closing time arrives, finish all transaction with customers, and have the security guard or a member of staff stand by the door to allow them to leave and then lock the door behind them.
- Lock all perimeter doors including the main entrance and any exit doors.
- Count cash in the manager's office - it should never be done in view of windows or customers.
- Complete inventory reconciliation reports
- The manager should perform a bag/coat check of exiting employees.
- Activate alarm system, turn off all lights, exit and secure the premises.
- Walk around the outside of the building and make a final check that all doors, windows and points of entry are secured.

Waste Disposal

Regular Waste Disposal Procedures

Our company is committed to recycling disposable waste whenever possible. The retail store generates waste from its usual business activities. In order to prevent diversion of our marijuana products by their removal with trash for later retrieval we have developed the following procedures.

- During the shift, all waste is to be placed in the storage container in the work room.
- The manager will help put the stored waste into disposal bags, ensuring that no inventory is included with the waste.
- During closing procedures (see above), the manager will bring the bag of waste outside to the dumpster.

Marijuana Waste Disposal Procedures

In the course of normal operations small amounts of marijuana waste may be generated from (for example) broken packaging, or customer returns. All marijuana waste must be disposed of in accordance with 935 CMR 500.105 (12).

- All marijuana waste will be placed in a ziplock bag and deposited into the locked disposal container for inventory at the end of the day. Each item for disposal must be weighed, recorded, and entered into the inventory reconciliation report.
- All waste will be held for seven (7) days
- At the end of the seven days the marijuana waste will be ground and mixed with other organic waste in a manner that renders the marijuana unusable for its original purpose and deposited at the local landfill.
- At least two licensed marijuana agents must witness and document this process.
- Such documentation shall be retained for a minimum of three years or longer if so directed by the Commission.

Storage, Inventory Control and Reconciliation

In accordance with 935 CMR 500.110 (1) all marijuana products at our retail store must be securely stored to prevent unauthorized access, loss, theft, and diversion. Inventory control protocols are designed to accurately account for all products that enter and leave the facility. All marijuana products arrive pre-packaged from our suppliers facility, where it has been weighed, packaged, labelled and bar-coded. Marijuana products are transported from the cultivation/manufacturing facility by state-licensed, secure transportation and are enclosed in a sealed container together with a shipment manifest.

- The store manager, in their role as security manager is responsible for opening the container, and matching the manifest to products contained within.
- In accordance with 935 CMR 500.105 (13) (a) the store manager must weigh each product item and ensure that it matches the manifest and is correctly labelled and bar-coded. The label must indicate the originating marijuana establishment name, address and registration name. The store manager must, in accordance with 935 CMR 500.105 (13) (c) note and record the name and registration number of the agent who prepared the manifest.
- The store manager must carry out this process in the presence of at least one other licensed marijuana agent.
- All products must be scanned and immediately entered into the retail store inventory.
- Any discrepancies must be **immediately** reported to Senior Management and documented.
- The container may only be opened in a designated secure area.
- The entire delivery arrival and unpacking process must be recorded on surveillance or video cameras to ensure the integrity of the chain of custody.
- The store manager signs the manifest and enters the new inventory into the “seed-to-sale” tracking software.
- The store manager stores all new inventory in its appropriate place in the vault and places the original manifest in the safe.
- Inventory is to be generally stored in the locked vault. Sufficient sales stock for each days business will be removed from the vault and stored on the shop floor. Should additional stock be required during the course of the day, the store manager will remove the required stock from the vault and add it to the sales stock on the stock floor.
- The vault door must be kept locked at all times and may only be opened to perform necessary tasks before being locked once more.
- At the end of each day, the store manager conducts an inventory of the sales stock and returns this to the vault for secure storage.
- Each day, the store manager must complete the inventory reconciliation report that documents what was sold during the day, and the store manager adds the manual count to the report. In the event any of the inventory has damaged packaging or is past its usable date, the dispensary manager moves this particular inventory to a storage container marked “Unusable Inventory”. The dispensary manager then updates the software to show what specific packages of marijuana products have been moved from the active database to the “dead” inventory file.
- When finished, the store manager must save the reconciliation report using the “seed-to-sale” tracking software. Variances between expected inventory and actual inventory must be **immediately** reported to Senior Management and documented.
- These reports are checked each day by our internal auditor. Unreported discrepancies will be flagged, documented and **immediately** reported to Senior Management.
- Each and every discrepancy will be personally investigated by Senior Management, or their deputy, within 24 hours.

- If there is no obvious explanation for the discrepancy, Senior Management will review the retail store's surveillance tapes for the week prior to the issue, and also review all sales and inventory reports produced by the Point of Sale system for the same time period.
- Senior Management will act on the inventory issue after documenting where the inventory went missing, and will interview the appropriate personnel to determine whether his or her conclusions are correct.
- In the event the inventory was taken by a store employee, they will be terminated and the police will be notified for possible prosecution.
- In the event the inventory was inaccurately counted, Senior Management will create a report stating such, and provide it to the board of directors. Senior Management will also review his or her findings with the store manager in order to flag any compliance issues and if necessary create new procedures to avoid the issue again.

Shipping and Transportation Security

The transportation of marijuana is one of the most vulnerable points for protecting inventory. Certain rules and protocol must be observed when receiving transported goods to insure the safety of the drivers, the customer, and the inventory.

- All transportation of marijuana, and marijuana products will be carried out by a state licensed marijuana company.
- All products will be appropriately tagged to ensure traceability back to the original plant, and all product must be logged in the computer system. Each container will be sealed and placed in a master container that will be video-taped, sealed and weighed at the facility where it leaving from.
- All product enclosed in the master container should be in a secure, lockable area in the specially-adapted vehicle.
- Deliveries will be scheduled in advance and the retail store will make staff available to ensure the safe and expeditious transfer of goods from the vehicle to the safety of the facility.
- Prior to the arrival of goods the Store Manager should ensure that exterior security lighting is functioning correctly.
- The Store Manager should conduct a brief counter-surveillance sweep for any suspicious activity within or outside the store facility
- The entire delivery process must be recorded on both video and surveillance cameras.
- The receiving process is as noted in *Storage, Inventory Control and Reconciliation*, above.

Incident Reporting

In accordance with 935 CMR 500.110 (7), senior management will notify appropriate law enforcement authorities and the Commission of any breach of security immediately upon discovery of the breach. Such incidents include, but are not limited to:

- Discovery of discrepancies during inventory
- Diversion, theft or loss of any marijuana product
- Any criminal action involving or occurring on or in the retail store premises
- Any suspicious act involving the sale, cultivation, distribution, processing or production of marijuana by any person
- Unauthorized destruction of marijuana
- Any loss or unauthorized alteration of records related to marijuana
- An alarm activation or other event that requires response by public safety personnel or security personnel privately engaged by the company
- The failure of any security alarm system due to a loss of electrical power or mechanical malfunction that is expected to last more than eight hours
- Any other security breach

Senior management will, within ten calendar days, provide notice to the Commission of any incident described in 935 CMR 500.110 (7) by submitting an incident report in the form and manner determined by the Commission which details the circumstances of the event, any corrective action taken, and confirmation that the appropriate law enforcement authorities were notified.

All documentation related to an incident that is reportable pursuant to 935 CMR 500.110 (7) will be retained by the company for not less than one year or the duration of an open investigation, whichever is longer, and made available to the Commission and law enforcement authorities upon request.

Security Procedures and Emergency Responses

All employees will be trained in our store's protocol for specific emergencies. It is imperative that we keep our customers and staff safe, and that we safeguard the inventory through our implemented security measures.

- Our security plan is designed to deter and prevent entry into, and theft from, restricted access areas containing marijuana products.
- All employees are responsible for ensuring that all doors to non-public areas are kept locked at all times unless there is an operational need for the door to be unlocked.
- The Store Manager is responsible for ensuring that any visitor be issued a "VISITOR" badge that must be clearly displayed during the entirety of their visit.
- Only visitors with a clearly defined need to enter non-public areas of the facility may do so. All visitors entering any area must be escorted by a member of staff at **all** times.
- Each visitor must present official or state-approved photo-ID, and sign our log book, stating time of arrival, purpose of visit, and time of departure. This must be done on each occasion, and each day of the individual's visit.
- Retail store employees must vigilantly observe the actions and behaviors of all customers while on the premises, and notify a supervisor if someone becomes disorderly, appears impaired, attempts to enter any part of the retail store designated for employees only, or exhibits any other suspicious behavior.
- Retail store employees must insure that all marijuana inventory remains in locked storage which is accessible only to other authorized members of staff.
- Each retail store employee must call over a supervisor to count out cash for a "drop" when their drawer has over \$500 in it. The manager will count the money, and both will initial the drop sheet with the time and amount being deposited.
- Retail store employees will check all locks, alarms, cameras and security equipment before leaving for the night.
- No keys may be handed over to allow access for doors, storage cabinets, etc. Designated keyholders must unlock limited access areas, wait and observe while necessary tasks are carried out by members of staff, and lock and secure the limited access area upon completion.

Armed Robbery Procedures

In the event of a robbery, there are four things that you must remember:

- Remain calm
- Remain alert
- Remain observant
- Comply with the robber's demands

The company values its employees and their customers first and foremost. Inventory can be replaced, cash can be replaced, but human lives cannot. **Remember - there is nothing in the store whatsoever worth dying for.**

- In the event of an armed hold-up, comply with all demands in a polite, courteous and efficient manner.
- Most perpetrators simply want to take the cash, and get out as quickly as possible. Follow the perpetrator's instructions and commands completely and without hesitation.

- Anyone near the silent alarm should activate it if they can do so without being detected. There should be no rapid, unexplained movements. If the opportunity arises that the employee is close enough to the alarm to push the panic button with their knee or to do it without being noticed, then do so with **extreme caution**.
- If the police show up while the perpetrator is still on the premises, and asks if someone tripped the alarm, the Retail Store Manager should simply say that the cameras are all monitored at the police station. **Never, ever, give any indication that someone alerted the police.**
- **Do not look into the robber's eyes, it will only heighten their anxiety about being recognized.** Our surveillance system will provide the police with the strongest identification of the perpetrator, so employees should carefully, if possible, attempt to recognize features of the robbers.
- If possible, tell the employees that they are to do everything the perpetrator asks.
- Open the cash registers, and then back away. Allow the robber unfettered access to the money, so they will take what they want and hopefully leave quickly.
- Avoid confrontation. This is not the time to engage the robber in small talk or to ask why they are doing this. There is no need for any sort of conversation that goes beyond "yes" or "no" unless asked for a specific answer by the perpetrator.
- If the robber demands the inventory, show them where it is in the front room, but do not point out the back room unless they demand to know. Open the storage locker for them, and back away.
- While the robbery is in progress, employees should make note of their physical characteristics - approximate height and weight, any sort of accent, distinguishing features such as scars or tattoos. If the perpetrator had a weapon was it held in their left or right hand? Was it a revolver, or a semi-automatic? Approximately how long was the barrel? Their clothing should also be observed - did they wear anything with a team insignia or brand name? Were they wearing any sort of brand name shoes or sneakers? Did they touch anything with an ungloved hand or commit any act that may have left DNA evidence behind (spitting, drinking, smoking).
- Once the perpetrator has left, do not attempt to follow them outside. Try to observe the make and model of the vehicle they left in, or the direction in which they ran. If possible, write down the license plate number. Remember, our parking lot is under camera surveillance, and hopefully the footage will provide sufficient evidence for the police to apprehend the suspects. Any other potential evidence should be left untouched and protected from tampering until police arrive.

After the Robbery

- Once the perpetrators have left, the police should be contacted as quickly as possible by any means available.
- Before the police arrive, obtain the names, addresses, and contact details of any witnesses to the crime. Request that they remain in the store until the police arrive. If they insist on leaving, ask for their contact information, but **do not attempt to block their way or in any way prevent them from leaving.**
- Meanwhile, If anyone has a medical issue, or states that they may be having a heart attack or some other medical episode, **call 911 immediately** and urgently request an ambulance for the individual. Any employee or customer with current CPR training should immediately attend to the individual and attempt to make them comfortable until the EMTs arrive.

- Secure the scene to preserve any evidence. Lock the doors, keep people away from the areas where the robbers were and keep any and all evidence that may have been left behind by the suspects.
- When the police arrive, answer all of their questions and provide them with any sort of contact information they request. Also, ensure that the Retail Store Manager has called Senior Management and that they are aware of what has occurred.

Inventory Theft and Diversion

- Inventory theft and diversion come in two primary forms - inside theft and outside theft. Inside theft occurs when an employee removes inventory without permission and without paying for it. Outside theft occurs when a non-employee steals an item(s) from the retail store. There is also a hybrid version when an employee collaborates with an outside person to steal inventory from the retail store.
- Our surveillance system is capable of recording all incidents, except those that happen in the bathrooms. However, theft is a crime of opportunity, and with employees it may occur when something is being moved, something is not given to a customer when it is paid for, or when an accounting or reporting error occurs and excess inventory is either brought to the retail store or is there after an inventory count.
- We have two ways to detect theft - actual observation, or inventory reports that indicate something is missing. If an employee observes a theft by another employee, they are obligated to bring it to the Store Manager's attention. The manager will observe tapes and inventory counts, and determine the correct course of action.
- When inventory is stolen by an outsider, the police and Senior Management are alerted, and the previous robbery procedures are followed in reporting the incident by senior management.

NO customer may enter our retail premises without first producing a valid, recognized, photo ID. Valid ID must be shown to security personnel at the entrance to the retail store and at the Point of Sale for data-entry purposes.

There are NO EXCEPTIONS to this rule.

Fire in Facility

The company has developed the following fire emergency plan that will be taught to, and practiced by all employees for implementation in the event of a fire on the premises.

- In the event of noticing smoke or a fire, activate the fire alarm and announce that the building needs to be evacuated.
- The Store Manager, if time allows, should move all inventory from the sales stock and cash from the registers into the vault and secure it (assuming that the vault is not the source of the fire in which case the door should be closed but not secured.) **This should only occur if the Store Manager does not see open flames, or smoke that is too dense to walk through.**
- The Store Manager, if safe to do so, should move through all rooms in the retail store, and ensure that everyone has made it out safely.
- Once outside, The Store Manager should verify that all members of staff are present.

- In the event the fire is small and containable, any of the many portable fire extinguishers located throughout facility may be used to attempt to tackle the fire. These should be used with extreme caution. **If the fire source is in or near an electrical enclosure do not attempt to tackle the fire.** Step away and continue evacuation procedures.
- Make sure the entrance to the facility is unobstructed allowing access for fire department vehicles. Ask anyone present who has parked in front of the facility to please move their vehicle immediately to facilitate access for the emergency services.
- When the fire department arrive, detail where you believe the fire started, and where it is the most intense.
- Inform Senior Management of the fire and the current situation.

REMEMBER THE ACRONYM “RACER”

R	Rescue people from the immediate area. Move people away from smoke and fire, and yell to insure the facility is empty.
A	Activate the nearest alarm, and contact 911 with the address of the facility. Provide your name, the location, the potential source of the fire, and stay on the line while they respond.
C	Contain the fire by closing all windows or doors if possible.
E	Extinguish the fire with an appropriate fire extinguisher for the type of fire being fought. Only do so if it does not involve any risk of life.
R	Relocate to a safe area. Make sure the store is cleared, and move people away from the entrance and any windows.

Information Technology Security

Our business is reliant upon certain software and hardware technologies in order to function efficiently and remain in compliance with local, State, and Commission requirements.

Our primary software systems may be summarized as follows:

- Point of Sale software (cloud-based)
- Seed-to-Sale tracking software (cloud-based)
- State-mandated METRC software (cloud-based)
- Accounting software (cloud based)
- General administrative software (cloud-based and locally stored)

Our primary hardware systems may be summarized as follows:

- Security system
- Point of Sale system
- Scanners, card, and barcode readers
- Printers
- Modems and Routers
- Local area network
- Laptop computers.

Many of these systems will contain restricted information. This restricted information is sensitive in nature, proprietary, and specific to our business. Unauthorized compromise or disclosure would likely have serious financial, legal, or regulatory impacts. Examples include personally identifiable data, credit card data, employee data, or computer system details. Restricted information is only available on a need-to-know basis.

Both the company and any computer service providers are required to comply with regulations designed to prevent access to, and loss of, sensitive and personally identifiable information from unauthorized disclosure and identity theft. Encryption is mandated by many laws and standards for some information transmission or storage.

Acknowledgement

In addition to the other agreements that may be required, acknowledgement of the Information contained within this document are part of the terms and conditions of employment with the company.

- Acknowledgement is required at the time of initial employment and annually thereafter.
- Where applicable, the store manager must ensure that all employees, visitors, and contractors have been provided with a copy of this Information Technology Security Protocol. Additionally, it is the responsibility of the sponsoring manager to ensure compliance with this and all the company Information Technology Security Protocols.
- Those employees whose job responsibilities require them to access credit card information will be required to participate in annual security awareness training.

Employee Administration

The store manager initiates the addition of new access by providing notification to senior management who administer IT security.

- Senior management updates the system with new hires and termination information. Store managers are responsible for notifying senior management when an employee, contractor or consultant is no longer associated with the company for any reason so that access can be disabled or removed.
- State-mandated pre-employment background checks are conducted on all employees regardless of whether their job responsibilities require them to access credit card information and other restricted data.

Contractors and Temporary Workers

Contractors must complete an agreement and be approved by senior management. Once a contractor has been approved, the store manager must work with senior management to confirm and ensure that access can be established.

Acceptable Use

The company's information and technology resources must be used in an approved, ethical, and lawful manner. Employees and contractors must always be alert to actions and activities they may perform that could breach company policies regarding the Internet, electronic mail, social networking and use of the company's computing resources.

All computer systems belong to the company and may only be used for business purposes. Company personnel should not have any expectation of privacy in anything they create, store, send, or receive via the the company computing environment. If users have any uncertainty on the appropriateness of their actions, they should clarify their understanding with their manager.

Equipment and Media Security

- Lost or stolen electronic devices must be reported to senior management immediately. This includes laptops, smartphones, or removable storage devices that contain company data.
- Strict control must be maintained over the internal or external distribution of any media that contains restricted information. Company information is limited to authorized users on a need-to-know basis and must not be copied, e-mailed, or printed without adequate physical controls.
- Contractors or consultants using personal equipment to conduct the company business are responsible for physically securing equipment in their possession that contains company-related information. Loss of equipment containing company information, even if personally owned, must be reported immediately to senior management.

Security Controls

- Senior management oversees the infrastructure and controls for centralized networks, servers, databases and desktop computers.
- Users must not disable, uninstall, or modify the security software, settings or encryption installed on laptops or mobile devices.

Security Logging and Monitoring

- Logs of key system events and access to sensitive information are in place and administered by senior management.
- Systems that provide initial entry/authentication into company networks and any application system that processes company information must be configured to capture security audit log data.

- Activities of those with privileged accounts (who have a higher level of access on servers or within applications) must also be captured and recorded in security audit logs.
- Logs are protected from unauthorized modification or destruction and are retained for a minimum of 180 days (six months) or as required.
- System or application administrators must routinely monitor system or application logs for anomalies regarding access to information. Exceptions must be investigated and appropriate action taken.

Third-Party Access

- Third-party (non-employee) access to the company's systems must be governed by formal written agreements or contracts. Network connections between the company environment and third parties must follow agreed-upon security procedures. These agreements may require signed Confidentiality and Non-Disclosure statements restricting the subsequent usage and dissemination of the company information.
- Vendors or other third parties with access to the company-owned or leased equipment or systems housed in a the company data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

Access Control

- Access to the company systems and applications is role-based and will be granted to authorized users based on job classification.
- Users are limited to the system capabilities they need based on job function or role and as authorized by management.
- The company computers are equipped with screensaver locks that will activate after 15 minutes of inactivity.
- Users must manually log off or lock workstations if they will be unattended prior to activation of the screensaver lock.

System and User Accounts

- Accounts are assigned to an individual and may not be shared.
- Guest accounts must be disabled if a system or application is provided with one.
- Vendor-supplied default accounts and passwords must be disabled or changed.
- System accounts, such as background accounts that are used for internal processing, are exempt from time-based password change requirements.

Passwords

- Passwords are confidential and must not be shared.
- Passwords must be changed on first use or if they have been reset for the user by senior management.
- Senior management and other administrators resetting passwords must verify the identity of all users requesting a password reset prior to performing the reset.
- The primary user Password must be changed at least every 90 days.
- Accounts used for system administration that have a higher level of privilege must also be changed every 90 days, or more frequently if the situation warrants.

Account Review

- Senior management or their designees must review the user accounts for the systems and applications they administer and verify the appropriateness of continued access. This review must be performed at least every twelve months.
- Access should be disabled immediately upon notification from a store manager or senior management that an employee, contractor, or consultant is no longer with the company.

Network Connectivity

- All devices should primarily access the internet through our LAN. WiFi use will be restricted certain limited devices only
- Senior management oversees the company's network, and all new wired connections must be requested through them.
- Wired devices, such as servers, that will be connected to the network must be approved and implemented by senior management for their respective networks.
- Employees and other authorized users must request remote access and use established connectivity methods to connect to the company networks from a remote location.
- Use of other remote connectivity methods is prohibited.

Changes to Applications

- Application change control is a security issue because unauthorized or accidental changes to applications may impact the integrity and availability of the data.
- The ability to change applications is limited to authorized users.
- Applications managed by senior management may not be changed without their permission

Application Security Standards

- If a third party is hosting an application, data protection controls provided by the third party must be adequate to meet regulatory and contractual requirements for security.

Security Incident Response / Disaster Recovery

Security Incident Response

- All users must report suspicious activities or actual occurrence of any unauthorized activities to the store manager who must, in turn, notify senior management.
- Notification should be made immediately or as soon as reasonably possible. This includes unauthorized use of accounts, logon IDs, passwords, loss of laptops or other devices, or potential breaches of the company computer systems and networks.
- Senior management will complete an Incident Report and conduct any investigation that may be required. Incidents that involve information compromise, such as a data breach or other loss of information, will be handled by senior management
- Senior management will work with law enforcement, IT consultants, and IT service providers to resolve the incident and ensure that correct notification procedures are followed.
- Users detecting potential information security events should immediately report them to the store manager

Business Continuity/Disaster Recovery

Business Continuity Plans are corporate plans that describe in detail how business areas will continue functioning in the event of a major system outage or a disaster. Senior management is responsible for documenting a Business Continuity Plan and designating a Business Recovery Coordinator who will develop and maintain their plan and participate in notification and recovery activities.

Disaster recovery plans describe how IT systems and resources will respond to a disaster situation and restore processing to the business based on the company's business objectives and timeframes for recovery of critical applications. Senior management will provide overall coordination and management in the event of a disaster, and assemble the necessary recovery and business teams to provide a timely response.

Backups

Company data is regularly backed up using defined business requirements for information recovery. Critical information should be stored on company-owned storage devices to ensure regular and automatic backup and recovery. Critical information should not be stored on personal computers or laptops, or on unencrypted personally-owned devices. If additional storage space is needed, contact the your supervisor for options

Compliance and Audit

Compliance with Legal Requirements

The Information Technology Security Program supports compliance with state and federal laws

Third Party Service Providers

Additional security protocols may be required for any third-party service provider that receives, stores, maintains, processes, or otherwise is permitted access to personally identifiable information provided to them by the company.

Whenever selecting and retaining any third party service provider, the company will:

- Take reasonable steps to confirm that the service provider is capable of maintaining appropriate security measures to protect personally identifiable information consistent with all applicable laws and regulations, and
- Require the service provider to contractually agree in writing with the company to implement and maintain such appropriate security measures.

Audit

Audit reviews may be conducted by an external state auditor and/or by IT consultants on a regular basis. Selected application security reviews may be performed as part of internal audit plans or general controls audits.

Enforcement

Those detecting violations of this ITSP must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to senior management, who will determine the extent of risk that any non-compliance condition presents and remediation activities that are required. Users who deliberately violate information security standards as

outlined in this document will be subject to disciplinary action up to and including termination from employment or association with the company.

Exceptions

Business needs may occasionally require variance from established Information Technology Security Protocols. A particular business function may not be able to be performed effectively, reasonably, or cost-effectively if the ITSP is followed. In these instances, senior management must be notified stating the underlying business problem and recommended approach or acceptable alternatives. Alternatives and any potential risks or problems the alternatives may cause will be considered. If a variance is granted, the affected Information Technology Security Standards will be updated and communicated.

COMMERCIAL LEASE FOR 246 COMMERCIAL STREET, PROVINCETOWN

This Lease is made as of the March 21, 2018 by and between Philip Swayze, having a mailing address of 33 Charlotte Street, Riverside, Rhode Island 02915, as Trustee of The Joel Newman Revocable Living Trust dated February 18, 2011, (hereinafter referred to as "Landlord") and "Hennep Property Holdings" having a mailing address of c/o Ciota Legal Group, 421-B Main St., Ridgefield, CT 06879 (hereinafter referred to as "Tenant") for property located at 246 Commercial Street, Unit 2, including approximately +/- 340 square feet, Provincetown, Massachusetts 02657 (hereinafter referred to as "Premises") upon the following terms and conditions:

1. Term and Rent:

Landlord agrees to rent the Premises for a term of one (1) year, beginning on April 1, 2018 (the "Lease Commencement Date") and terminating on April 1, 2019. The amount of rent shall be thirty thousand dollars (\$30,00.00), payable in four installments of seven thousand five hundred dollars (\$7,500.00) beginning at the "Lease Commencement Date", with an option to renew (see section 4). All rental payments are payable without set-off or deduction, without notice, and all payments shall be made payable to "The Joel Newman Trust" dtd 2/18/11. Annually at the Lease Commencement Date, the rent shall be adjusted based on the consumer price index.

2. Permission to Sublet:

For the term of this lease, Landlord agrees that Tenant shall be permitted to sublet the Premises to "Hennep" having a mailing address of c/o Andrew Koudijs, 130 St. Mary's Street Boston MA 02215. No other parties will be permitted this sublet without expressed written permission from Landlord.

3. Early Termination:

Tenant or Landlord may terminate the lease with sixty 60 days written notice. These failures are not restricted to but include non-payment of rent, damage to the property. Termination by Tenant within the signed lease term between March and October will require full payment for the following quarter's rent regardless of occupancy. Termination outside of these dates requires a sixty day (60) notice and payment of all rent while the property is occupied.

4. Option to Renew:

Tenant may renew this Lease for an additional two years, but must exercise this option in writing to Landlord not later than sixty (60) days prior to the end of Lease term (“Option Deadline”). If Tenant fails to exercise this option by the Option Deadline, then this option shall be considered null and void.

5. Security Deposit:

Landlord shall hold Tenant’s security deposit in the sum of two thousand and five hundred dollars (\$2,500.00) as security for the performance of Tenant’s obligations under this Lease, including, without limitation, the surrender of possession of the Premises to Landlord as herein provided. If Landlord applies any part of the deposit to cure any default of Tenant, Tenant shall, on demand, deposit with the Landlord the amount so applied so that Landlord shall have the full deposit on hand at all times during the term of this Lease. The security deposit may also be used to cover any unpaid utilities or outstanding rent that has not been paid.

6. Utilities:

Tenant is responsible for the management and payment of all utilities except water and hot water. Upon acceptance of lease terms, existing accounts belonging to the premises shall be moved into Tenant’s name. Upon lease termination, the electric (Eversource) shall be turned over to Landlord fully paid to the end of the lease.

7. Water/Sewer/Rubbish/Recycling/Property Taxes:

Landlord is responsible for all costs associated with local and federal property taxes, the water and sewer usage of the property and for all costs associated with the disposal of rubbish and recycling generated in the normal course of business of Tenant.

Tenant is responsible for bagging rubbish or putting recyclables in appropriate recycling containers, and complying with all recycling ordinances. Items may be placed in an area that is shared with the Provincetown Bookshop located at 246 Commercial Street, as long as they are taken out on the designated days of the week.

Any trash or recycling that exceeds a normal week of doing business may require the Tenant make special arrangements with the Town of Provincetown. These costs will be the Tenant’s responsibility.

8. Telephone and Internet:

Tenant shall be responsible for the installation, termination, and all associated expenses of any telephone and/or internet system(s).

9. Use:

Tenant shall use and occupy the Premises as a retail establishment, or for any other use approved in writing by the Landlord. Tenant agrees to comply with all reasonable requests made by Landlord to maintain Tenant's Premises in a visually appealing condition so that Tenant's Premises does not represent a visual detriment to the property or infringe on the commerce of co-tenants in the building. Tenant shall, at all times, provide appropriate lighting and obstruction-free window space that displays an orderly and presentable interior space. No merchandise will be displayed on the street in front of the Premises or inside the walkway to the Premises without prior written permission from the Landlord.

10. Care and Maintenance of Premises:

Tenant hereby acknowledges that the Premises are in good order and repair, unless otherwise indicated herein. Tenant shall, at his own expense and at all times, maintain the Premises in good and safe condition, including plate glass, and shall surrender the same at termination in as good condition as received, normal wear and tear accepted. Landlord shall not be responsible for repairs except for the roof, exterior walls, and structure of the building and grounds, which are to be maintained by Landlord. If Tenant is open during the winter months, Tenant is responsible for keeping the entry and sidewalks clear of snow and ice.

11. Rest Room Facilities:

Tenant has unrestricted access to a designated storage space and exclusive use of a bathroom just outside the Premises. Tenant must maintain bathroom cleanliness and is responsible for keeping it stocked with supplies. This bathroom is NOT to be made available to the general public.

12. Music:

Tenant may play music in the leased premises as long as the music does not become a nuisance or excessive to patrons and other tenants in Landlord's sole judgment. Tenant is responsible for paying any ASCAP, BMI or other music licensing fee.

13. Signage and Alterations, Soliciting/Advertising:

The Tenant shall not, without first obtaining the written consent of Landlord, make any alterations, additions or improvements in, to, or about the Premises. Tenant shall submit to Landlord, for Landlord's written approval, Tenant's proposal for signage in or about the Tenant's Premises. Tenant is responsible for researching and conforming to any applicable town bylaws and regulations. Landlord must approve all signage in advance of its display. The Premises has the ability to hang a sign over the street due to a Provincetown grandfathering clause due to the history of signage over the last several decades.

There is to be no soliciting, no merchandise, artists, entertainers or vendors, no sandwich boards in front of the building or inside the building unless approved in writing by the Landlord.

14. Equipment:

Tenant will supply Tenant's own store equipment. Said items shall not be considered fixtures and shall be removed at the end of the tenancy by Tenant and should not in any way damage the Premises upon said removal.

15. Ordinances and Statutes:

Tenant shall comply with all statutes, ordinances, and requirements of all municipal, state, and federal authorities now enforced, or which may hereafter be enforced, pertaining to the Premises, occasioned by or affecting the use thereof by Tenant. Landlord shall comply with all statutes, ordinances, and requirements of all municipal, state, and federal authorities now enforced, or which may hereafter be enforced, pertaining to the Premises.

16. Hours of Operation:

Tenant is encouraged to keep regular business hours, whether Tenant's business is seasonal or year-round.

17. Parking:

There is no parking associated with this property.

18. Assignment and Subletting:

Other than permissions set forth in section 2 of this Lease, Tenant shall not assign this Lease or sublet any portion of the Premises without prior written consent of the Landlord. Any such assignment or subletting without prior written consent shall be void and, at the option of the

Landlord, may cause this Lease to be terminated.

19. Entry and Inspection:

Tenant shall permit Landlord or Landlord's agent to enter upon Premises at reasonable times and upon reasonable notice for the purpose of inspecting the same, and will permit Landlord at any time within sixty (60) days prior to the expiration of this Lease to place upon the Premises any usual "to let" or "for lease" signs, and permit persons desiring to lease the same to inspect the Premises thereafter.

20. Possession:

If Landlord is unable to deliver possession of the Premises at the commencement hereof, Landlord shall not be liable for any damage caused thereby nor shall this Lease be void or voidable, but Tenant shall not be liable for any rent until possession is delivered. Tenant may terminate this Lease if possession is not delivered within thirty (30) days of the commencement of the Lease term hereof.

21. Indemnification of Landlord:

Landlord shall not be liable for any damage or injury to Tenant or any other person associated with Tenant's business, or to any property occurring on the rented Premises or any part thereof, and Tenant agrees to hold Landlord harmless from any claims for damages, no matter how caused.

22. Insurance:

Tenant shall, at his own expense and at all times, maintain public liability insurance including bodily injury and property damage insuring Tenant and Landlord as an additional insured with minimum coverage as follows: One Million and 00/100 dollars (\$1,000,000.00) for any one occurrence and Two Million and 00/100 dollars (\$2,000,000.00) general aggregate. Landlord shall be named as an additional insured in such insurance. A Certificate of Insurance shall be delivered to Landlord by postal mail to 33 Charlotte Street, Riverside, Rhode Island 02915 or by e-mail to philip.swayze@gmail.com. The Certificate of Insurance shall provide for a minimum ten (10) day written notice to Landlord in the event of cancellation or material change in coverage. To the maximum extent permitted by insurance policies, which may be owned by Landlord or Tenant, Tenant and Landlord, for the benefit of each other, waive any and all rights of subrogation which may otherwise exist.

23. Eminent Domain:

If the Premises or any part thereof or any estate therein, or any part of the building materially affecting Tenant's use of the Premises, shall be taken by eminent domain, this Lease shall terminate on the date when title vests pursuant to such taking. The rent, and any additional rent, shall be apportioned as of the termination date and any rent paid for any period beyond that date shall be paid to Tenant. Tenant shall not be entitled to any part of the award for such taking or any payment in lieu thereof, but Tenant may file a claim for any taking of fixtures and improvements owned by Tenant, and for moving expenses.

24. Destruction of Premises:

In the event of a partial destruction of the Premises during the term of this Lease, from any cause, Landlord shall forthwith repair the same, provided that such repairs can be made within sixty (60) days under existing Governmental laws and regulations, but such partial destruction shall not terminate this Lease, except that Tenant shall be entitled to a proportionate reduction of rent while such repairs are being made based upon the extent to which the making of such repairs shall interfere with the business of Tenant on the Premises. If such repairs cannot be made within said sixty (60) days, Landlord at his option may make the same within a reasonable time, this Lease continuing in effect with the rent proportionately abated as aforesaid, and in the event that Landlord shall not elect to make such repairs which cannot be made within sixty (60) days, this Lease may be terminated at the option of either party. In the event that the building in which the demised Premises may be situated is destroyed to an extent of not less than one-third of the replacement cost thereof, Landlord may elect to terminate this Lease whether the demised Premises be injured or not. A total destruction of the building in which the demised Premises may be situated shall terminate this Lease. In the event of any destruction or damage due to natural disaster, the Tenant is solely responsible for any damage to Tenant's merchandise.

25. Default and Landlord's Remedies on Default:

A. If Tenant vacates the premises, or if the Lease is terminated because of Tenant's default in the performance of Tenant's obligations hereunder, the Landlord shall not be required to make reasonable effort to re-let the Premises for the best rent obtainable. In the event that the Landlord does relet the Premises, and if rent received by the Landlord from such reletting (after deducting the cost of advertising and broker's commissions, if any) equals or exceeds the rent payable hereunder, the Tenant shall not be liable to pay such rent. If the rent received by Landlord from such reletting, after such deductions, is less than the rent

payable by Tenant hereunder, Tenant shall be liable for the deficiency and expenses of alterations, if required. In any event, Tenant shall forfeit the rents paid in advance.

- B.** If Tenant defaults in the payment of rent, or in the performance of any of Tenant's obligations hereunder, the Landlord may, at any subsequent time, declare the term ended; reenter the Premises, or any part thereof, with or without legal process, remove Tenant or any part occupants, and fully repossess the Premises. Landlord shall also have the right to collect by Summary Proceedings, or otherwise, any rent due and unpaid, and further right, at any time, to collect and receive any rent due without thereby affecting the service of notice, commencement of suit, or final judgment for possession of the Premises and unpaid rent.
- C.** The granting herein to Landlord or Tenant, or the exercise by Landlord or Tenant, of any right or remedy or of any alternative rights or remedies, shall not affect or prejudice any other rights or remedies the Landlord or Tenant may have.

26. Attorney's Fees:

In case suit should be brought for recovery of the Premises for any sum due hereunder, or because of any act which may arise out of the possession of the Premises, by either party, the prevailing party shall be entitled to all costs incurred in connection with such action, including reasonable attorney's fees.

27. Waiver and Notice:

No failure of Landlord to enforce any term hereof shall be deemed to be a waiver. Any notice which either party may or is required to give, shall be deemed given by mailing the same, postage prepaid, to Tenant at the address specified above, or to Landlord at the address specified above, or at such other places as may be designated by the parties from time to time.

28. Heirs, Assigns, Successors:

This Lease is binding upon and inures to the benefit of the heirs, assigns, and successors in interest to the parties.

29. Subordination:

This Lease is and shall be subordinated to all existing and future liens and encumbrances against the property.

30. Entire Agreement:

The foregoing constitutes the entire agreement between the parties and may be modified only by a writing signed by both parties. The following exhibits, if any, have been made a part of this Lease before the parties' execution hereof.

31. Governing Law:

This Lease shall be construed in accordance with, and governed by, the laws of the Commonwealth of Massachusetts, without giving effect to rules governing choice of law

32. Execution:

This Lease may be signed in multiple counter-parts.

IN WITNESS WHEREOF, the said parties have hereby set their hands and seals as of the date first written above.

LANDLORD: The Joel Newman RLT dtd 2/18/11

By: _____
Philip Swayze, Trustee

TENANT: Hennep Property Holdings

By:  _____
Paige Koudijs
 _____

30. Entire Agreement:

The foregoing constitutes the entire agreement between the parties and may be modified only by a writing signed by both parties. The following exhibits, if any, have been made a part of this Lease before the parties' execution hereof.

31. Governing Law:

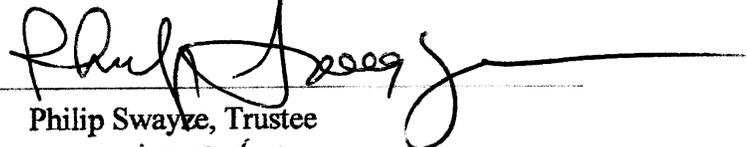
This Lease shall be construed in accordance with, and governed by, the laws of the Commonwealth of Massachusetts, without giving effect to rules governing choice of law

32. Execution:

This Lease may be signed in multiple counter-parts.

IN WITNESS WHEREOF, the said parties have hereby set their hands and seals as of the date first written above.

LANDLORD: The Joel Neyman RLT dtd 2/18/11

By: 
Philip Swayze, Trustee
3/22/18

TENANT: Hennep Property Holdings

By: 
Paige Koudijs
3/16/18