Safety and Security Plan 1

Security Personnel Summary 1

Security and Surveillance Features Summary 3

Security Floor Plan 5

Plans for the Storage of Cannabis and Cannabis Items 5

Diversion Prevention Plan 6

Emergency Management Plan Summary 6

Procedures for Screening, Monitoring, and Performing Criminal History Record Background Checks of Employees 7

Cybersecurity Procedures Summary 8

Workplace Safety Plan Summary 9

History of Workers' Compensation Claims and Safety Assessments 10

Safety and Security Plan

Puffsie, LLC will enact and oversee safety and security procedures in accordance with (NJAC §17:30-9.10, §17:30-9.11 and §17:30-9.12 (pages 150-154).

Security Personnel Summary

Security employees report to the Security Manager. They are tasked with the responsibility to observe the facility, premises and parcel, to control access to the facility, and respond to emergencies. All security employees are expected to know and uphold the policies and procedures in this Safety and Security Plan. Security employees will wear identification badges, abide by rules related to access to the premises and individual rooms, maintain appropriate discretion regarding company operations, and otherwise act in a way that preserves the safety of the facility and others.

The Security Contractor is a third-party company that will be hired to provide professional uniformed and unarmed security personnel for the facility who are certified per the Security Officer Registration Act, P.L.1939, c.369 and P.L.1971, c.342. The Security Contractor will be selected by the CEO and will report to the Security Manager The Security Contractor will provide basic training, uniforms, and human resources services to the security employees. The Contractor will provide services supplemental to the in-house security employees, such as off-hours video and alarm surveillance as required by NJAC § 17:30-9.10(c) (page 150), neighborhood and premises car and foot patrols, and oversight of valuable product transfers.

Security Manager
The Security Manager (SM) is an employee of the company, and is responsible for carrying out the bulk of the responsibilities identified in the Security Plan and managing security employees. Responsibilities include, but are not limited to:

- Implement and enforce security policies and regulations in accordance with NJAC §17:30-9.10, §17:30-9.11 and §17:30-9.12.
- Implement appropriate security and safety measures to deter and prevent the unauthorized entrance into areas containing cannabis and the theft of cannabis, in accordance with NJAC § 17:30-9.10(b)(2) (page 150).
- Implement security measures that protect the premises, consumers and cannabis business personnel in accordance with NJAC § 17:30-9.10(b)(2) (page 150)
- Ensure all security equipment and systems are operated and maintained according to manuals, standard security practices, and requirements of NJAC §17:30-9.10.
- Establish a protocol for testing and maintenance of the security system in accordance with NJAC § 17:30-9.10(b)(4) (page 150).
- Administer the access and visitor management system, in accordance with company policies and NJAC § 17:30-9.4(l) (page 139).
- Ensure the protection of people, property, and assets.
- Reduce risks, respond to incidents, and limit liability in all areas of financial, physical, and personal risk.
- Act as liaison to the local Police Department (PD).
- Schedule all security services and officers.
- Manage a budget covering security resources and employees.
- Compile security-related reports as required by the Executive Team.
- Utilize all security systems to discover security breaches and identify compliance issues.
- Train employees according to established security procedures and conduct regular security meetings to ensure full understanding and implementation of security policies and procedures.
- Ensure the maintenance of security training records and logs.
- Act as liaison to all departments on security policies, procedures and incidents.
- Coordinate the security of product transfers in and out of the building.
- Conduct security evaluations to ensure ongoing compliance with policies and procedures.
- Ensure the proper reporting and documentation of all incidents and provide initial information for investigations to the CCO.
- Ensure that all security records are forwarded properly according to the Recordkeeping Plan.
- Foster a spirit of cooperation, respect and professionalism among employees and other managers.
- Stay up to date on security-related issues and trends by means of periodically reviewing the literature, becoming a member of one or more related organizations, participating in conferences, and/or other means of networking with and learning from other security experts.

Requirements:
- At least 21 years of age
- 5-10 Years Security Management Experience

- Minimum of high school diploma or equivalent, college degree preferred
- Certified per Security Officer Registration Act, P.L.1939, c.369 and P.L.1971, c.342
- Ability to pass a background check
- Has not been dishonorably discharged from the military

Security Personnel, Unarmed
Security employees report to the Security Manager and assist in maintaining the safety and security of the staff, products, and the facility. Responsibilities include, but are not limited to:

- Conduct periodic inspection of premises to protect against fire, theft, vandalism, and illegal activity.
- Maintain required records and logs.
- Prevent access to any unauthorized persons within the registered premises
- Assist any staff with security access issues.
- Monitor any suspicious behavior by guests, visitors, or personnel.
- Ensure compliance with state and local regulations and company procedures.
- Prepare reports as requested by the Security Manager.

Requirements:

- At least 21 years of age
- Certified per Security Officer Registration Act, P.L.1939, c.369 and P.L.1971, c.342
- High school diploma or GED
- Has not been dishonorably discharged from the military

Security and Surveillance Features Summary

The company will install a security alarm system and digital video surveillance system in accordance with NJAC § 17:30-9.10(b) (page 151) that, in accordance with NJAC § 17:30-9.10(c) (page 153), will be continuously monitored, 24 hours a day, seven days a week. In accordance with NJAC § 17:30-9.11 (page 153), law enforcement and neighbors located within 100 ft. of the property will be provided with an emergency contact name and phone number of a facility supervisor to whom they can report problems with the establishment during and after operating hours.

Alarm System

- The alarm system will be purchased, installed and operated in accordance with NJAC § 17:30-9.10(b) (page 150).
- The alarm system will cover the property perimeter, the fence around the facility, and both the exterior and interior of the building.
- All doors that provide access to the building will be alarmed, as well as rooms with exterior windows, skylights or access points on the roof, the main office, and other rooms that contain vaults, safes, or stored product.
- The alarm system will be installed, commissioned and monitored during non-business hours by a vetted, licensed alarm company that is capable of meeting all state and local regulations.
- The entire security system, including the alarm system, will have battery-powered backup that will be instantly triggered by the failure of utility-supplied power, in accordance with

NJAC § 17:30-9.10(b)(1) (page 150). The backup batteries have the power to maintain the electrical requirements of the security system for 72 hours.

- The alarm system will be equipped with a backup power supply and a failure notification system that operates in accordance with NJAC § 17:30-9.10(b)(1) (page 150). The failure notification system will immediately send an electronic alert to designated company officers, as well as to the appropriate police department, alerting them of the loss of primary electrical support for the system.
- The Security Manager will conduct testing and preventative maintenance inspections on the security system, including the alarm system and backup power system, every 30 days and will promptly implement all necessary repairs necessary to ensure continued ongoing proper operation of the system, in accordance with NJAC § 17:30-9.10(b)(5) (page 150). All instances of security system testing and maintenance will be logged on the Security Equipment Testing & Maintenance Log.
- In accordance with NJAC § 17:30-9.10(b)(6) (page 150) In the event of a security system outage that is expected to last more than 8 hours, the Security Manager will notify the Commission pursuant to NJAC § 17:30-9.11 (page 153) and provide alternative security measures approved by the Commission or close the authorized physical addresses impacted by the failure or malfunction until the security alarm system is restored to full operation. [NJAC §17:30-9.11(b) states that the company should notify the CRC by phone within 24 hours and by email within 5 business days notifying the agency of the outage and the corrective measures taken.

Video Surveillance System

Puffsie, LLC will install a digital video surveillance and recording system, in accordance with NJAC § 17:30-9.10(b)(9) (page 150). This system will provide remote viewing access to the Commission and be approved by the CRC before license issuance. Critical activity areas that will be surveilled include, but not limited to:

- The front and rear of the premises
- Parking areas
- The exterior within 20 feet of all doors and windows to the outside not adequately covered on the front or rear sides
- The entrance area, such that all people who enter the building are clearly recorded
- All locations where sales occur
- All locations where product transfers take place
- All locations where products are on display or are stored
- All locations where individuals interact with the product, including shipping and receiving areas
- Areas such that individuals who are opening safes or vaults can be clearly viewed
- Areas used for the destruction and disposal of cannabis items
- All other rooms that require a higher level of access to enter

The video surveillance system, in accordance with NJAC § 17:30-9.10(b)(9)(i) (page 150), will be set up to be in working order at all times, utilizing backup power in the case of utility outages, and monthly testing and maintenance procedures to ensure proper functioning of the system and prevention of mechanical failures. It will include electronic monitoring, cameras and panic buttons, as needed to meet regulatory requirements and protect the facility, the premises,

personnel and visitors. In accordance with NJAC § 17:30-9.10(b)(10)(ii) (page 150), the company will ensure that the video surveillance system will be supported by adequate security lighting, which, at a minimum, will illuminate all entrances and exits.

Recorded Surveillance Storage
In accordance with NJAC § 17:30-9.10(b)(9)(ii) (page 150), The original tapes recorded by the video surveillance system will be stored in a locked cabinet in the executive offices for a minimum of 30 days.

- Backup copies of at least the most recent week of surveillance footage will be stored on a secondary secured server on the property or, if on removable media, off-site in a vault or safe where it is easy to access and easily reproducible.
- Video will be made available immediately upon request to state and local law enforcement and regulatory authorities, and to other entities as required by law.

Security Equipment Testing & Maintenance
- The SM or his designee will be responsible for overseeing the proper implementation of an equipment testing and maintenance SOP and activity log in accordance with NJAC § 17:30-9.10(b)(5) (page 150).

Facility Access
In accordance with NJAC § 17:30-8.1(f) (page 133) All employees, vendors, contractors, or others operating on behalf of the company will possess their Cannabis Business Identification Card at all times on the business premises. A badge version of this will be made that will remain visible on the outer clothing of the person that includes:
- The company's name
- The employee's name;
- The date of issuance and expiration
- A photograph of the employee or contractor

In accordance with NJAC § 17:30-8.2 (page 135) The company will notify the Commission within 10 business days of the date that a qualified person pursuant to paragraph (a) of NJAC § 17:30-8.1 (page 133) ceases to work at or be affiliated with the cannabis business or testing laboratory. In accordance with NJAC § 17:30-9.4(l) (page 139), all visitors will be accompanied at all times by an escort who, on behalf of Puffsie, LLC is a holder of a Cannabis Business Identification Card. This requirement includes Vendors, Contractors and their employees who do not possess individual Cannabis Business Identification Cards.

Plans for the Storage of Cannabis and Cannabis Items

All finished cannabis/cannabis items will be stored in a locked climate-controlled vault or storage room located in a Restricted Access Area, and only be accessible in accordance with NJAC 17:30-9.12 (page 154). Personnel will ensure that:

- Authorized visitors are constantly overseen if they must work in or pass through cannabis storage areas.

- Each batch of a product is stored separately and distinctly from other batches of products on the premises.
- A storage label with the following information is physically attached to the container of each batch:
    - The date of entry into the storage area
    - The unique identifiers and batch number associated with the batch
    - A description of the products with enough detail to easily identify the batch
    - The weight or quantity of units in the batch
    - The best-by, sell-by, or expiration date of the batch, if any
    - Any other required information
- If a label must be modified, a Label Modification Form must be filled out and submitted to a Manager.
- If any products are removed from the storage cabinets, destroyed, or transferred for any reason, the required information related to the transfer or destruction of goods will be entered into the inventory control system, and the regulating authority will be notified.
- No one may remove products from the secure storage room without having an approved operational reason for doing so and following the inventory control procedures.

Diversion Prevention Plan

The company is aware of the importance of regulatory concerns related to the security of cannabis/cannabis items. Theft and diversion prevention are among our highest priorities as a compliant and successful cannabis business. The company has established policies and procedures to avert the possibility of diversion of cannabis/cannabis items. The procedure for Anti-Diversion can be found in the separately submitted Inventory Control, Storage, and Diversion Prevention SOP. A summary of the policies follows:

- A minimum of two (2) authorized employees must be present when making deposits or withdrawals of cannabis and/or cannabis items or cash into designated storage and/or vault rooms.
- Storage rooms and vaults are always monitored by multiple security monitors and systems, overseen 24 hours per day by the Security Manager on duty.
- Restricted Access Areas are clearly marked, secured, and always monitored.
- Security checks are in place at the main employee entrance and product transfer points to ensure unauthorized individuals do not gain access to the facility and its restricted areas. Security checkpoints are monitored by video surveillance at all times.

Emergency Management Plan Summary

In compliance with 29 CFR 1910.38, Puffsie, LLC will have written (required if more than 10 employees) or oral (an option if 10 or fewer employees) emergency action plans. Plans will cover how to report fire or other emergencies, alarm systems, evacuation, critical operations, who to contact for more information, training and how the plans will be periodically reviewed. These will be easily accessible and kept at the workplace, both in electronic and paper format. The Facilities Manager is responsible for implementing the Emergency Management Plan and communicating with emergency responders. The company has an extended version of its Emergency Management Plan that will be summarized here. The key points are ensuring that:

- A well-functioning alert/alarm/notification system is in place

- Cannabis/cannabis plants/cannabis items, cash and important records are locked, if possible, before leaving during evacuations.
- An Evacuation Plan is in place that is properly documented and rehearsed by all personnel.
- Proper incident reporting and record keeping is done after the event

The types of emergencies that are addressed are:

- Fires
- Storms/Floods
- Medical Emergencies
- Robberies/Burglaries
- Earthquakes
- Chemical Spills
- Hazardous Gas Emissions
- Power Outages

Procedures for Screening, Monitoring, and Performing Criminal History Record Background Checks of Employees

Screening

Prospective employees will be screened for employment using the following techniques:

- Request of resumes that include, a minimum, job experience, educational background and professional references
- Use of preliminary internal assessments to screen out those applicants who do not demonstrate the minimum requirements in their application submissions
- Verification of the applicants employment record and educational status
- Verbal verification of a sufficiently clean criminal record to qualify for the position
- Contacting the supplied professional references to obtain detailed information about the performance of the applicant in previous job positions.
- Social media scan to find further information on the applicant that might not have been supplied by the above.

If all of the initial screening steps are found to be sufficiently positive, Puffsie, LLC will then conduct a video conference interview with the applicant. The applicant will be asked why they have left previous jobs, if they have left under good terms and given the required amount of notice, and what kinds of problems they have had with previous co-workers and employers, among other more informal questions oriented around getting to know the person and assessing if he/she is a good match for the position. If all of these steps are passed with sufficient satisfaction, the prospective employee will be asked to fill out an application and supply written consent and payment, if appropriate, for a background check.

Background Checks

The CRC requires all prospective cannabis business employees to pass a background check conducted by the Company in accordance with NJAC 17:30-7.12 (page 153). Official background checks are conducted through the MorphoTrak/IdentiGo state-sanctioned system, and require the person to submit fingerprints. When conducting a third-party background check on a prospective employee, company will collect the following information from the person:

- The person's name and signature
- Copy of a state or federally issued ID
- A statement affirming that the employee has not been convicted of any disqualifying offenses
- Written permission from the employee to conduct both the third-party background check and the official MorphoTrak/IdentiGo background check.
  Any false information or failure for the person to comply with the above will result in permanent disqualification from employment.

Employee Monitoring
Once hired, employees will be monitored by video surveillance cameras as part of the video monitoring system for the facility's Restricted Access Areas. Personal areas such as bathrooms, breakrooms, and locker rooms will not be monitored. The company will have a policy of not allowing employees access to personal email accounts from the workplace, or from using personal cell phones on the job. This mitigates the theft of intellectual property, prevents distraction from work, but also protects the employee from inadvertent recording of personal information that might be automatically gathered by the company's cybersecurity system. This is discussed further in the following section on Cybersecurity. Employees will not be audio recorded on the job without consent.

Cybersecurity Procedures Summary
In accordance with NJAC § 17:30-9.10(a) (page 150), the company will protect its electronic and computer systems from tampering, and hence from theft or diversion of cannabis. Primarily, ensuring proper and limited access to the Inventory Tracking System software will be prioritized, to prevent tampering with inventory data in a way that could obscure the diversion of cannabis/cannabis plants/cannabis items.

The technology and information assets of the company are made up of the following components:
- *Computer Hardware* - CPUs, disks, email/web/application servers, and PC systems
- *System Software* - operating systems, database management systems, backup/restore software
- *Application Software* - Custom written applications, customized third-party applications, and unaltered third-party applications
- *Communications Network Hardware and Software* - routers, hubs, modems, switches, firewalls, etc.

Classification of Information
User information and company information found in computer system files and databases will be classified as *confidential* or *non-confidential*.
Examples of confidential data include:
- Cannabis/cannabis item inventory data
- Classified financial information
- Customer data
- Cannabis plant and product data
- Vendor information

- Formulas, procedures, and other intellectual property

The CCO is responsible for reviewing and approving the classification of information to determine the appropriate security level designation. Security Levels will be divided into 3 levels--high, medium and low and access will be limited and controlled accordingly.
Employee Cybersecurity Policies include the following topics (detailed further in the full-length Cybersecurity Plan):

- Acceptable use of network and systems
- Use of personal devices on the company network
- Email security
- Password management
- Transferring data
- Remote network use
- Company monitoring of employee activity
- Disciplinary actions

The IT/Security Manager will be responsible for implementing the Cybersecurity Incident Handling SOP. In the event of a cybersecurity breach, the procedures is as follows:

1. Assess the scope of the incident. Investigate alerts from active security tools and acknowledge any new detections.
2. Isolate affected endpoint(s) from the network to prevent malware from moving laterally throughout the environment.
3. Kill running process(es) associated with malware.
4. Delete any identified malicious codes.
5. Block any IP addresses appearing to be involved with the attack.
6. Remove any suspicious persistence mechanisms (Scheduled Tasks, Autorun Keys, etc.).
7. Minimize risk of a future attack by assessing administrative controls. Review account usage and reset passwords, limit administrative access where possible, and disable unnecessary file sharing access.
8. Patch vulnerable systems.
9. Mark relevant detections and alerts as remediated.
10. Identify and document the scope and severity of the damage
11. Complete Incident Report
12. Notify Supervisor/s, as required, to report the incident, its scope/damage and all further recommended steps for repair and prevention from future similar attacks.

Workplace Safety Plan Summary
OSHA workplace safety rules do not specifically address cannabis workplace safety due to federally illegality, but the following topics are relevant (described in detail in our full-length Workplace Safety Plan, available upon request):

- Electrical Hazards - 29 CFR Part 1910.137, 29 CFR Part 1910 Subpart S, 1910.331, 332, 333, and 1910.335
- Personal Protective Equipment - 29 CFR Part 1910.132 and 29 CFR Part 1910.134
- Exposure to Hazardous Gasses - 29 CFR Part 1910.1000 and 29 CFR 1910.165

- Flammable Liquids - 29 CFR Part 1910.106
- Hazard Communication - 29 CFR Part 1910.1200
- Hazardous Energy (Lockout/Tagout) - 29 CFR Part 1910.147
- Injury and Illness Prevention Program - 29 CFR 1960.40, 29 CFR 1910.132(d), 29 CFR 1910, Subpart I, Appendix B, 29 CFR 1904, 29 CFR 1960.29
- Covid Prevention Protocols - OSHA's Covid Guidance
- Point of Operation and Machine Hazards - 29 CFR 1910.212
- Pressurized Gases - CGA P-1 (1965), C-6 (1968), C-8 (1962), S-1.1 (1963 and 1965 addenda), and S-1.2 (1963)
- Slips, Trips, Falls and Ladders - 29 CFR 1910.21 and 1910.22 & 23

History of Workers' Compensation Claims and Safety Assessments

Puffsie, LLC has no experience here.