



Design 710 LLC, Medical Marijuana Permittee No. 02172023
Design 710’s Application for a Class 5 (Dispensary) Adult Use Permit
SECURITY AND SAFETY PLAN

INTRODUCTION

Design 710, LLC (“Design 710”) is a certified Women-Owned (WBE) Business currently operating in Atlantic City at 112 Park Place as a medical marijuana dispensary. Design 710 submits this Security and Safety Standard Operating Procedure for the purpose of implementing its policy relative to compliance with *N.J.A.C.* 17:30 §§ 12.2(d) & (e), 12.3, and 12.8, and in connection with its Class 5 Retail Adult Use Permit Application.



Design 710 has prepared this Security and Safety Plan for the dispensing of marijuana in full compliance with the New Jersey Cannabis Regulatory, Enforcement Assistance, and Marketplace Modernization Act, *N.J.S.A.* 24:6I-31, et. seq., and the accompanying regulations including but not limited to *N.J.A.C.* §17:30-7.8, §17:30-9.10, and §17:30-12.7.



As a currently permitted and operational medical marijuana dispensary at 112 Park Place in Atlantic City, Design 710 is pleased to present its current operating procedures and policies as further evidence of its mission to operate a safe, secure, compliant, and successful Class 5 marijuana facility. Design 710 has already met with Chief Sarkos and several officers from the Atlantic City Police Department, gave them a tour of the space and provided them complete access to the dispensary’s surveillance system.

Design 710 just hasn’t dreamt and written a Safety and Security Plan, it lives it every day as outlined below.

PLAN ADMINISTRATION

The following outlines the general roles and responsibilities of the Security Plan administration:

Title and Role	Security Plan Area of Responsibility
Facilities Manager	Ensures the physical security of cannabis.

Safety & Security Director	Ensures all employees follow security policies and procedures; security training with the Human Resources Officer; meets with law enforcement regarding alarm responses, criminal activity, and ensures the security of hardware, software, data, and communications networks.
General Manager	Ensures employee training and compliance.
All Employees	Aid in the security of the Facility; immediately report security breaches and incidents of non-compliance to their supervisor or the Security Director; receive training.

PERSONNEL PLAN

All employees must successfully complete mandatory foundational training prior to working at Design 710. In addition, employees will undergo annual and quarterly performance reviews to foster healthy communication and growth. Design 710 is a drug and smoke-free workplace with an employee assistance program under N.J.A.C. §17:30-9.9.

RISK MANAGEMENT POLICIES AND PROCEDURES

The following policies and procedures will be implemented during employee orientation as risk management guidelines:

- Health and Safety Policy;
- Infection Control Policy/Manual;
- Incident Reporting Policy;
- Complaints Management Policy;
- Product Handling Policy;
- Emergency Plans; and,
- Zero Tolerance Policy.

Every employee will be provided an employee handbook for their own personal reference to further ensure compliance with CRC regulations and company policies.

SECURITY STAFF

Design 710’s Security Director, George Shick, is a retired Atlantic City Police Officer who spent 26 years on the Force before becoming Security Manager at The Botanist’s Medical Marijuana Dispensary in Atlantic City. Design 710’s current security team numbers three (3) employees, including George, and we will expand the unit as we move towards the summer season.



Design 710 has contracted with PS^x, a New Jersey-licensed private alarm contractor which installed commercial grade security equipment and provides professional monitoring services at our currently operating medical marijuana dispensary. N.J.A.C. §17:30-7.8 and §17:30-9.10.

DIVERSION PREVENTION & SECURITY TRAINING

We know that having a trained and educated workforce is paramount to an effective diversion strategy. Therefore, Design 710 devotes a considerable amount of time, resources, and energy to ongoing diversion prevention and security training. At a minimum, and in compliance with the Act and rules, specifically N.J.A.C. §17:30-7.8 and §17:30-9.10, the diversion prevention and security curriculum includes the following:



- Proper use of security measures and controls that have been adopted by us for the prevention of diversion, theft, or loss of cannabis;
- State and local laws, regulations, ordinances, and guidance;
- Procedures for reporting incidents or security concerns to supervisors;
- Employee and visitor access procedures;
- Camera monitoring and safety systems;
- Suspicious behavior and incident identification;
- Safe storage of cannabis;
- Incident management and reporting;
- Risk assessment and response;
- Cybersecurity and Data Protection;
- Regulatory inspection preparedness and law enforcement interaction; and
- All other topics as specified by the New Jersey Department of Financial and Professional Regulation (“Department”).

Diversion prevention and security trainings are mandatory for every new employee and will be conducted within 30 days of hire. Additionally, each employee will be required to participate in quarterly continuing education trainings on diversion prevention. Employees will be given real world examples of diversion and taught the appropriate response. Teaching the material through problem solving, discussion, and feedback will empower and increase understanding and retention of the training. This process of integrating knowledge will develop a culture of shared values, perspectives, and become the way of daily conduct and purpose at the dispensary facility.

To assist with our security training, Design 710 has a contract with Jim Sherrard, owner and operator of J Sherrard Inc., a cannabis consulting firm. Jim is a retired Lieutenant of the New Jersey State Police where he served 25 years before joining the New Jersey State Medical Marijuana Program at its inception as an original investigator. Following his time with state program, Jim acted as national security director for Curaleaf for seven (7) years before striking out on his own.

Jim meets monthly with Design 710 managers and employees to provide security updates and tips as to what trends are occurring in the industry as well as provides feedback as to the current state of operations to ensure all known and unknown threats are understood.

DISPENSARY SECURITY INSPECTIONS

A security officer and the Facilities Manager perform or oversee a daily opening inspection to ensure compliance with the rules set forth by the CRC and all applicable state and local laws, regulations, ordinances, and other requirements. The Facilities Manager will remain a safe distance away from the facility entrance while the security officer enters and conducts a walk-through of the facility to be certain it is safe to enter. The security officer will signal the Facilities Manager that he or she may enter. Areas of inspection include, but are not limited to, ensuring the facility and all critical areas are sanitary and safe; all areas are secured; exterior and interior lighting is

operational; and all security equipment is in good working order. Any areas not compliant will be noted and directed to the Facilities Manager and executive team. The development of a corrective action plan, delegation of duties, and the mandated expedience of such corrective actions will be determined by the Facilities Manager. A security officer and the Facilities Manager will also perform or oversee a daily closing inspection to ensure: All cannabis-infused products are properly accounted for in the inventory management system and stored securely; All security systems are functioning; All doors are secured; and All persons have left the building. The Security Director and Facilities Manager will maintain close relationships with the Atlantic City Police Department in order to provide the local authorities all of the information it needs to ensure the safety and security of the community is maintained.

PHYSICAL SECURITY

Design 710 will have a state-of-the-art security system that utilizes commercial grade equipment. As required by N.J.A.C. 17:30-9.10, Design 710 will conduct maintenance inspections and tests of the security alarm system at intervals not to exceed 30 days. All security equipment, cameras, alarm systems, and locks will: (1) be kept in good working order, (2) has been installed by a commercial, licensed service provider, and (3) be tested no less than twice per year (in addition to the 30 day security alarm tests).

SPECIFICATION FOR THE SECURE PRODUCT STORAGE VAULTS AND TWO SAFES

All marijuana products including edible lozenges, pills, oils, topicals, tinctures, liquids, and flower/dry plant will be stored within the locked, restricted-access, secure product storage room. Only a management-level employee will have access to entry codes that will unlock the vault. Entry codes will be changed every 30 days to enhance security. The product vault will be connected to Design 710's integrated electronic video management system and controlled access systems for monitoring and record keeping purposes.



Marijuana products are stored in a custom steel-reinforced concrete vault designed to UL TL-30 standards with a UL 768 Group 1 electro-mechanical combination lock. The storage vault will be built to withstand abuse for 30 minutes from mechanical/electrical/hand/picking tools, grinding points, carbide drills, cutting wheels, and power saws. Design 710's UL Group 1 combination lock will have over 1M possible combinations and be resistant to skilled attacks up to 20 hrs.

SECURE DOOR LOCKS

Doors will feature UL 437-rated Medeco Locks which are drill proof, require multiple diamond blades to cut, cannot be picked open, and cannot be duplicated without Medeco-issued credentials and unique authorization codes. Only the security personnel and management, and necessary authorized employees will have access to the Medeco-lock keys, which will never leave the dispensary.



Medeco Classic CLIQ Deadbolt

ENTRY AND EXIT POINTS

Design 710 will use the 734 Wiegand Interface Module by Digital Monitoring Products, Inc. or its equivalent for entry and exit electronic access control equipment, including:

- All doors will be 18-gauge hollow metal, or similar burglary-resistant material, with commercial-grade I, non-residential locks;
- Electric strike locks on all doors in the facility with an override option for emergency exit
- RFID proximity card access control on all doors to restricted areas and all exterior doors;
- RFID proximity card access control devices for all doors accessing a limited access area;
- Access control system allowing for programming individual user permissions and allowed entry times, as well as operations-specific information, e.g., employee photos;
- Access control system that identifies and monitors those entering and exiting; and, a backup battery system that immediately provides power for at least 24 hours.

LIGHTING

Outside perimeter of the Facility, including the parking lot, is well-lit by commercial metal halide fixtures sufficient to facilitate surveillance. Per N.J.A.C. 17:30-9.10 exterior lighting is designed not to disturb neighbors. Exterior lights at all entry & exit points remain constantly illuminated for recording. Lighting on the outside perimeter allows night vision cameras to record activity. Motion detecting lights will be installed in areas that are entered and exited infrequently. Motion sensors will be installed using the professional series Anti-Mask Motion Sensors on the interior, including above the ceiling tiles. Glass-break detection will also be used.

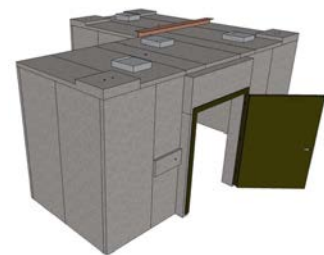
WINDOWS

All exterior windows at the Facility will have shock sensor alarms and motion detectors. The entrance vestibule will have a bulletproof service window facing into the mantrap.

VAULTS/STORAGE

As per the requirements of N.J.A.C. 17:30-9.10 and 9.12(b), all marijuana in the Facility that is prepared for sale shall be stored securely in compliance with 21 C.F.R. 1301.72. To prevent diversion, theft or loss, all marijuana will be securely stored in an approved UL-listed walk-in Class 5 Rated vault with a Class 5 vault door with security features that comply with all applicable requirements of 21 C.F.R. 1301.72(a)(3). All approved vaults will be kept securely locked and protected from entry and include the following features:

the walls, floor, and ceiling are constructed of at least eight inches of reinforced concrete or other substantial masonry reinforced vertically and horizontally with #4 ½-inch steel rods tied six 6-inches on center, or UL-listed modular vault panels; the door and frame unit are UL-listed burglary-resistant. Upon attempted unauthorized entry, it will transmit an alarm to Design 710's alarm monitoring service provider. Complete electrical lacing of the walls, floors, and ceiling, sensitive ultrasonic or infrared sensors within, a sensitive sound accumulator system, or other such devices or equipment designed to detect unauthorized entry and holdup buttons will be placed at strategic points of entry to the perimeter area of the vault. The vault's electrical alarm system will be a certified UL approved system.



ALARM SYSTEM

In accordance with the requirements of N.J.A.C. 17:30-9.10(b), Design 710 will have a professionally monitored security alarm system, utilizing commercial grade equipment, installed at the Facility, including the perimeter. The interior and exterior of the premises will be equipped with electronic monitoring, video cameras, and panic buttons. The alarm system will (1) provide protection 24 hours per day, 7 days per week, (2) send immediate or automatic notification to State or local police upon unauthorized breach of security, and (3) include a backup system that (a) activates immediately when electricity is lost, and (b) issues automatic or immediate notice to state or local police upon the loss of electrical support. Monitoring of the alarm system will be done 24 hours a day, 7 days a week and inspected/tested quarterly.



All alarm panels have a duress alarm function with a specific code to alert law enforcement and the security monitoring company that they are being forced to disable the alarm system. There are panic alarms throughout facility to create audible notice that there is an emergency situation that requires safety personnel or law enforcement response. Staff working with vendors, contractors, or the public will be required to wear a wireless transponder allowing for manual initiated or “man-down” feature. This feature is activated when the transporter is tilted more than a pre-programmed angle limit, triggering an automatic voice dialer requesting dispatch from law enforcement.

These provisions are accomplished by installing a UL listed, commercial grade, state of the art, intrusion system. It will manage the arm/disarm keypads for the facility, will have the capability to process alarms and events by individual point ID or zones, and report those events (by point ID) to a “Central Station” for dispatch of emergency personnel. The intrusion system will be monitored on site and off site by PS^x, the UL Listed Central Station Monitoring Facility.

The intrusion system keypads will have the ability to send a silent “duress” signal to PS^x. An employee can disarm the intrusion system with an alternate keypad code, triggering the duress signal to the Central Station. The intrusion system has the capability to accept multiple zoned input devices such as push buttons, foot rails, palm buttons, etc. These input devices can be programmed for either silent (hold-up) or audible (panic) operation. They can also integrate with the CCTV system for camera call up, as an aide to an operator in the security command center.

REDUNDANCY

Integral to the intrusion system is a digital communicator. The communicator will send emergency signals by event type and location (point ID) to PS^x for dispatch from a pre-recorded voice message. Transmission method is by a combination of phone line, IP based signaling, and/or cellular to assure redundancy in case one of the transmission paths should fail.

The security system control panels has supervisory capabilities that can detect conditions that might impact its ability to function. Such conditions include loss of primary power, low back battery, cut or “jumpered” wiring, equipment tampering (i.e. cabinet door opened or cover plate is

removed, loss of one of the communicators transmission paths, etc.) The system can also monitor facility equipment that could impact security operations such as a failure of the backup generator, sprinkler system trouble, or HVAC malfunction(s). Upon detecting a fault, the system can be programmed to sound locally on premise or communicate to PS^x. Notification features of the alarm system(s) include a “voicemail broadcasting system” that uses a prerecorded voice message to request dispatch from a law enforcement or emergency services.



INTRUSION SYSTEM

Electronic Circuit and Broken Magnetic Contact Detection

PS^x will wire all points of entry into buildings using electrically sensitized strips of metallic foil or wire. Any action that breaks the foil or wire breaks the electrical circuit and activates an alarm. It will also be equipping all doors and windows with magnetic contact switches, which activate an alarm when the door or window is open.

Infrared Motion Detection

This photoelectric detection system derives its name from the use of a light-sensitive cell and a projected-light source. The source transmits invisible light beams at several thousand pulses per second, and the cell receives them. An infrared filter over the light source makes the light beam invisible to intruders. When an intruder crosses the beam, the light beam breaks contact with the photoelectric cell, which activates an alarm. Crisscrossing light beams via hidden mirrors are effective within 500 feet.

30 Second Entry/Exit Delay

The alarm system features a 30-second entry and exit delay that provides the dispensary manager and security guard opening or closing the facility a brief period to enter or exit the facility before the alarm activates. While some systems may have delays up to 120 seconds, a shorter delay helps to prevent any unauthorized entry or criminal activity.

Sound Detection

Sound protection is part of our Vault Security system. This system uses supersensitive microphone speaker sensors installed on walls, ceilings, and floors to detect any sound caused by attempted forced entry.



Vibration Detection

The vibration detection is on all exterior windows of the facility and will also be part of our Vault Security system, this type of system is similar to the sound detection system. PS^x has placed vibration-sensitive sensors to walls, ceilings, and floors of the vault.

Back-up Systems

To guarantee uninterrupted security within the facility, 2 independently wired intrusion systems are installed. The 2 systems run independently and notify if there is an issue within the facility. It also allows for a back-up in the event one of the intrusion system goes off-line.

Design 710 will ensure the surveillance system is well maintained, inspected and tested annually. The Security Director will perform monthly inspections. **All** inspections and maintenance will be logged digitally and stored via our physical server with an additional encrypted cloud back-up by AWS for a period of 4 years. Management and security employees will be trained to identify, report and address any observable system problems. At no time will the system be permitted to operate while lacking any functionality. The Security Director, CEO and COO are the only persons permitted to make alterations or upgrades to the surveillance system.



Additional features of the surveillance system include:

- Email Alerts;
- Remote Backup;
- Online Viewing through a Web Browser;
- USB Backup;
- iPad, iPhone, and Android Apps;
- Junction Boxes – To prevent exposed cables of outdoor cameras; and
- 30 Frames per second

Security system maintenance will be performed quarterly by PS^x. When upgrades, repairs or maintenance are needed the Department, State and Atlantic City Police will be notified. Any testing that results in the system being down longer than 8 hours will be reported. Design 710 will institute an alternative security plan if it is down utilizing its security staff and local law enforcement. The facility will close to maintain integrity and safety.

FAILURE NOTIFICATION SYSTEM

The alarm failure notification system will provide phone, e-mail or text message alerts within five minutes of a system failure to the designated security personnel within the facility. If a system failure occurs during non-working hours and no security personnel are on site, the failure notification system will send notification to the Security Director.

CYBER INTRUSION DETECTION SYSTEM

Design 710's intrusion detection system (IDS) is a type of security software designed to automatically alert managers when someone or something is trying to compromise information system through malicious activities or security policy violations. IDS works by monitoring system activity through examining vulnerabilities, the integrity of files, and conducting an analysis of patterns based on known attacks. It automatically monitors the Internet to search for any of the latest threats.

There are three primary components of IDS:

- Network Intrusion Detection System (NIDS): This does analysis for traffic on a whole subnet and will make a match to the traffic in a library of known attacks.
- Network Node Intrusion Detection System (NNIDS): This is similar to NIDS, but the traffic is only monitored on a single host.

- Host Intrusion Detection System (HIDS): This takes a “picture” of an entire system’s file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.

PANIC BUTTONS



A panic button is a strategically placed or hidden button that automatically alerts police to an emergency situation. These buttons are small and are placed in a discreet location under the retail counter. It’s important that all buttons are in locations where employees will likely be present. If a robber yells “freeze” an employee should be able to quickly hit the button without anyone noticing. On duty police in the area will be dispatched immediately.

SURVEILLANCE SYSTEM

Design 710 installed a fully operational electronic surveillance system at its Facility. Monitoring of the surveillance system is done 24 hours a day, 7 days a week by Design 710’s security department and third-party professional security company PS^x. The surveillance system covers the interior and exterior areas of the Facility and, at a minimum, consist of the following:

- 4K High-Resolution Internet Protocol Cameras with Infrared technology;
- Equipment necessary to video record activity inside and outside the Facility;
- Appropriate equipment to record keycard and biometric entry and exit activity;
- A backup battery system; and
- A dedicated safe or vault to store all entry/exit records and video recordings.

Further, Design 710 has given the Atlantic City Police Department full and complete unrestricted access to its surveillance system which enhances its security protocols and provides for immediate response as needed.

VIDEO SURVEILLANCE EQUIPMENT

Surveillance equipment consists of digital/network video recorders with a record rate of a minimum 12 frames per second; High Resolution Video cameras with a minimum resolution of 1.3 megapixels; video cameras capable of identifying activity occurring within twenty feet from all points of entry and exits into and out of the exterior of the Facility; 4K video cameras with True Wide Dynamic Range for Facility interior; capabilities to produce a clear, color still photograph from any camera image; two monitors for remote viewing via telephone lines in State offices.

SURVEILLANCE COMMUNICATION

The surveillance system includes a failure notification system that alerts the Security Director of any interruption in surveillance and/or the failure of the monitoring system. The alarm will signal the Security Officer on duty when an unauthorized entry is attempted, showing the picture ID of the individual attempting entry on the access control monitor.

SURVEILLANCE TESTING

Design 710 will ensure that the surveillance system is properly maintained for playback quality so that the identity of all individuals and activity in surveillance areas are captured. All security equipment will be in good working order (with repairs made as soon as possible) and will be

inspected and tested at regular intervals, according to Design 710’s protocol, at least every 30 calendar days.

SURVEILLANCE SYSTEM RECORDS AND RECORDINGS

Design 710 maintains surveillance system records and recordings in the Facility and copies stored on a secure cloud storage with at least a 30-day archive. Video surveillance recordings will be stored on a server-based 8TB Network Video Recorder. This system will be a password-protected and separate from any other equipment in the Facility. The files and video surveillance recordings will be available for immediate viewing by the CRC or its authorized representative upon request.

DATA ARCHIVING

The challenge with any cloud-based data archiving resource is to ensure that it satisfies HIPAA’s data archiving requirements. Design 710’s data archiving and recordkeeping function is by Sceptre, Inc. Technologies (SIT), an information technology consultancy based in Glenside, Pennsylvania. SIT has developed and implemented a comprehensive protocol such that inactive records will be archived using Amazon Glacier, which is part of Amazon Web Services.



Amazon Glacier is a secure, durable, encrypted cloud storage service specifically designed for long-term record archiving. Designed to deliver 99.999999999% durability, Amazon Glacier supports the HIPAA-compliant recordkeeping initiatives of major healthcare organizations such as Orion Health and Cambia Health Solutions. Amazon Glacier supports “query-in-place functionality”, which permits analytics modeling on archived data.



SIT has implemented application protocols to ensure that Design 710’s inactive records, reports, and surveillance video files automatically transfer into the Amazon Glacier cloud program. All records will be kept according to HIPAA regulations and SIT will be retained long-term to monitor performance and compliance in the Restricted

Access Area under lock.

SECURE CLOUD STORAGE

A second, independent security system will be used to protect Design 710’s secure cloud storage system. This secure cloud storage system will be access-limited through passwords and monitored for unauthorized changes and will comply with the rules set forth by the CRC and applicable law.



ACCESS CONTROL

Design 710 will have comprehensive access control procedures to deter and prevent unauthorized entrance into the Facility and its restricted and limited access areas. Access to the Facility will be limited to Design 710’s employees, qualifying consumers, and authorized visitors.

EMPLOYEE ACCESS

No person is permitted to begin work at Design 710's Facility prior to physically receiving their Facility identification card or relevant confirmed registration with the CRC authorizing employment at the Facility. At all times, while on the facility premises, all employees must conspicuously display their New Jersey CRC issued Agent Identification Card that clearly identifies them to the public, including their position at the facility.

ACCESS CREDENTIALS RETURN

When an owner, principal, officer, director, board member, or employee ceases to work at or be affiliated with Design 710, their employment authorization expires immediately. In that case, Design 710 shall notify the CRC within 10 business days of the date of such expiration.

OSHA AND DESIGN 710 REPORTING

Occupational Safety and Health Act (OSHA) Compliance Plan
New Jersey does not have a state-adopted OSHA Act, so the Federal OSHA Act applies to Design 710's safety and health in the workplace. Design 710 has a Compliance with OSHA Checklist and will be using the OSHA Small Business Handbook or compliance. Design 710 will employ MaintainX (or equivalent) computerized cloud-based facility management/maintenance software ("CCMS") for all equipment maintenance, repairs, accidents, corrections, and task assignment. The Operations Manager will ensure the discipline or termination of any person contributing to operational negligence, that the facility possesses adequate liability insurance or an adequate self-insurance escrow at all times and the facility remains compliant with Americans with Disabilities Act ("ADA") guidelines.

Comply with the OSH Act's General Duty Clause and OSHA Standards

- Determine employer and employee coverage under the Occupational Safety and Health Act (OSH Act)
- Provide a workplace free from serious recognized hazards and comply with standards, rules, and regulations issued under the OSH Act, consistent with the OSH Act's general duty clause. For more information about the OSH Act's general duty clause, see Practice Note, Health and Safety in the Workplace: Overview: The General Duty Clause.
- Examine workplace conditions to ensure they conform to applicable Occupational Safety and Health Administration (OSHA) standards, including:
 - general industry standards; and
 - standards applicable to construction, maritime, and agriculture operations.
- For more information about specific health and safety standards promulgated by OSHA, see Practice Note, Health and Safety in the Workplace: Overview: Specific Safety Standards and OSHA Requirements.
- Make copies of OSHA regulations and standards available to employees on request.
- Determine whether the employer is covered by an OSHA-approved state plan and, if so, become familiar with the state's requirements. For information about states with their own occupational safety and health plans approved by OSHA, see Practice Note, State Occupational Safety and Health Plan Laws Chart: Overview.

Comply with Required Workplace Postings

- Post the OSHA poster (or the state plan equivalent) informing employees of their rights and responsibilities at a prominent location in the workplace. For a copy of this poster, see OSHA, Job Safety and Health: It's the Law Poster. For links to state law posters, see Practice Note, State Occupational Safety and Health Plan Laws Chart: Overview.
- Post the Summary of Work-Related Injuries and Illnesses (OSHA Form 300A) on February 1 of each year and maintain this posting for three months.
- Comply with workplace labeling and other requirements where employees may be exposed to toxic substances or harmful physical agents in the workplace.
- Post citations and documents showing a violation was corrected where applicable.

Establish an Injury and Illness Recordkeeping Procedure

- Establish a procedure for employees to report all workplace injuries and illnesses promptly and accurately that is:
 - reasonable; and
 - does not deter or discourage a reasonable employee from accurately reporting a workplace injury or illness.
- Inform each employee:
 - of the employer's reporting procedure;



Safety rules are designed to provide employees with knowledge of the recognized and established safe procedures that apply to many of the work situations encountered while employed at Design 710. We will maintain a Health and Safety in the Workplace Policy to ensure that we are complying with requirements. Design 710 will utilize the OSHA Inspection Checklist in the event of an OSHA inspection.

FIRE SAFETY

Design 710's dispensary complies with all local fire codes. Flammable materials will be stored in a fire cabinet properly labeled for first responder identification and all areas of egress will be properly signed in accordance with NFPA 704 standards. Fire extinguishers will be maintained annually and employees trained in fire prevention and mitigation measures.



WALKTHROUGH AND CLOSING

The General Manager or their designee must perform a daily walk-through to ensure compliance with Design 710 policies and procedures. The Daily Walk-Through Log record must be made after completion of the final walk-through each day. Each Manager is responsible for the daily

completion of the Daily Walk-Through Log and the timely response to any issues uncovered by the walk-through.

EMERGENCY AND INCIDENT RESPONSE POLICIES AND PROCEDURES

Design 710 has implemented incident response procedures addressing incidents that may occur, including, but not limited to natural disaster, unauthorized access, theft, or data security breach. Procedures comply with the rules set forth by the CRC and all applicable state and local laws, regulations, ordinances, and other requirements. Procedures for general emergency and incident management, containment, and corrective measures will be thoroughly detailed. The Security Director will ensure the appropriate response procedures are followed. Design 710 will maintain and make available all documentation related to an occurrence that is reportable in accordance with the regulations governing dispensing organizations. We will also develop sufficient additional safeguards in response to any special security concerns, or as required by the CRC, as well as any additional security as needed and in a manner appropriate for the community where our facility operates in accordance with N.J.A.C. §17:30-7.8 and §17:30-9.10.



INCIDENT REPORTING

Anyone with knowledge or a reasonable suspicion of an incident will be instructed to make an immediate report to one of our security officers or the Security Director. The person reporting the incident will complete an Incident Log. A security officer or the Security Director will collect the following information:

- Date and time of occurrence or suspected occurrence;
- Names and contact information of parties involved and any witnesses;
- Description of incident;
- Completed Suspect Description Forms, if applicable; and
- Any evidence supportive of the event (unless law enforcement is required on scene or enroute).

The Security Director will draft the Post-Incident Report and distribute it to the Chief Operations Officer (“COO”), Chief Compliance Officer (“CCO”), and the Chief Executive Officer (“CEO”) for review. The Security Director will ensure the appropriate employees are assigned to any follow-up actions. The Security Director will document the completion of all follow-up actions in the Post-Incident Report and distribute an updated copy to the parties referenced above.

NOTIFICATION

In compliance with N.J.A.C. §17:30-7.8 and §17:30-9.10, we will promptly document and report any diversion, loss, or theft of cannabis from our facility to the Atlantic City Police and the CRC. In addition, we will notify the CRC, and law enforcement authorities as appropriate, upon becoming aware of any unauthorized destruction of any cannabis and any loss or unauthorized alteration of records related to cannabis or purchasers. Such notice will be provided no later than 24 hours after discovery of the incident by way of a signed statement which details the circumstances of the incident, including an accurate inventory of the quantity and brand names of cannabis diverted, stolen, lost, destroyed, or damaged and confirmation that the local law enforcement authorities were notified.

We will also notify the CRC by telephone and email no later than the next business day, followed by written notification no later than 5 business days, of any of the following: An alarm activation or other event that requires response by public safety personnel; A breach of security; The failure of the security alarm system due to a loss of electrical support or mechanical malfunction that is expected to last longer than eight hours; and Corrective measures taken, if any. We will also report other incidents to the CRC, including, but not limited to:

- Breach of our network servers;
- Threats of violence to Design 710, employees, or visitors;
- Bomb threats;
- Any criminal activity;
- Civil disturbances;
- Hazardous chemical spill;
- Infectious disease epidemic;
- Serious accidents;
- Fires;
- Floods;
- Windstorms or tornadoes;
- Earthquakes;
- and
- Other acts of God.

INCIDENT CONTAINMENT

The Security Director, in coordination with the Facility Manager, will determine and implement the appropriate activities and processes required to quickly contain and minimize the immediate impact to personal safety, the facility, and other affected parties.

EVACUATION PROCEDURES

The Facility Manager, in coordination with the Security Director, may determine the need to evacuate. In the event of an evacuation, the Security Director will ensure that all employees and visitors on the premises, if applicable:

- DO NOT gather in lobbies;
- DO NOT open a door without first checking for heat;
- DO NOT touch any suspicious items or suspected bombs;
- DO NOT run or panic;
- DO NOT re-enter the building until authorized; and
- DO assist disabled individuals or others who need assistance.

The following corrective procedures may be required to return conditions to a normalized and secure state: Change all security codes; Replace locks and issue keys only to authorized employees; Ensure any video of the incident is archived; Restore security devices and/or apparatus to working condition; Repair any physical damage to the facility; Provide employees and visitors, if applicable, counseling, as needed; Perform a security re-training as soon as possible; and Modify Employee Access Control Log as deemed appropriate.

INTERNAL THEFT/ROBBERY PROCEDURES

In the event a threat is present to persons, the premises, or product inventory due to internal theft or burglary, employees will be trained to: Identify missing or compromised assets; Gather, remove, recover, and secure sensitive materials to prevent further loss or access; Power down, recycle or remove security equipment known to be compromised; Where possible, secure the premises for possible analysis by the CRC and law enforcement; Gather and secure any evidence of illegal entry for review by the CRC and law enforcement; Where possible, record identities of any party who might be a possible witness to events; and Preserve video recordings and Visitor logs for review by the CRC and law enforcement.

DISPENSARY COMPLIANCE: INVENTORY CONTROL, STORAGE, AND DIVERSION



Design 710's approach regarding implementation of an inventory management process is to develop controls that address CRC requirements under N.J.A.C. §§17:30-9.11, 17:30-9.12, 17:30-9.13, and N.J.A.C. 17:30-12.7, and include quality assurance and auditing features. Design 710 will implement inventory control procedures that utilize an Electronic Inventory Tracking System from Metrc, the CRC's approved seed-to-sale tracking software

provider. Design 710 will log, verify, and monitor the receipt of marijuana products, dispose of marijuana waste and facilitate the recall and return of defective marijuana.

CYBERSECURITY AND DATA BREACH PROTECTIONS

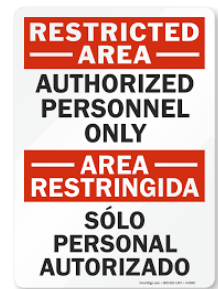
New Jersey requires any business which maintains, stores or manages computerized data containing personal information to notify State residents affected by a data breach without unreasonable delay under the Breach of Personal Information Notification NJ Identity Theft Prevention Act, P.L. 2005, c.226 and N.J. Stat. § 56:8-163 Notification Obligation. To safeguard its electronic



records, Design 710 has coordinated a plan with third-party IT and security vendor SCI to establish a data breach response plan which includes establishing a Response Team to handle data breach incidents. The Response Team will consist of the Safety & Security Manager; CCO and General Counsel who will perform: Incident Assessment – Determine when and where the data breach took place, as well as what data may have been compromised; Analysis – Analyze the affected system to determine if there are further weaknesses that may be exploited and review any issues that may have caused the breach; Communications Plan – Immediately notify the CRC of the suspected breach and determine the best method for notifying and communicating with affected individuals including consumers, physicians, staff, and third party vendors, with all notifications to begin within 24 hours of a detected breach; and, Law Enforcement – Notify local, state and/ or federal law enforcement if the nature of the breach requires it.

STORAGE

All marijuana products are securely stored out of sight in a temperature-controlled, locked and impregnable vault within a room in a Restricted Access Area of the facility which is under alarm and surveillance controls 24/7. Utilizing state-of-the-art technology that tracks and monitors all individual movement throughout the facility and electronic key cards to restrict unauthorized access, areas of storage will feature two (2) separate, secure, locked rooms: one secure room will be utilized to store all regular, sellable inventory that can be legally dispensed to qualifying consumers. The other secure room will store all products that are expired, damaged, deteriorated, mislabeled, contaminated, recalled, or whose containers or packaging have been opened or breached, as required by §§17:30-9.12 and 17:30-12.7.



CASH HANDLING AND COUNTERFEIT DETECTION

CASH HANDLING – EMPYREAL LOGISTICS

Design 710 is under contract with Empyreal Logistics to provide cash pick up services for the dispensary. Empyreal Logistics, an approved and preferred vendor for Design 710's bank BCB Bank, has assembled a team of tenured professionals who have built strong relationships with all types of industries including, financial service providers and retailers all across the U.S. Empyreal's team is comprised of a dedicated group of professionals with real-world experience in all areas of banking, logistics including cash management, compliance, transport and processing solutions, with added knowledge of highly-regulated, cash-intensive markets.



Empyreal will provide all cash pickup and delivery services for Design 710.

COUNTERFEITING

Each point of sale ("POS") center will be outfitted with portable counterfeit currency detectors. This will allow selected and/or questionable currency to be confirmed at the time of sale. The operational SOP for the POS system will outline the usage of the counterfeit currency detector use.



Inventory procedures will also include the counting, storage, and facilitating of funds transferred to and from the company. Funds will be managed by employees trained to receive, deliver, count, sort, document, and securely store cash, checks, and other methods of payment. Money will be accounted for via multilevel auditing and secure accounting procedures. Funds will be counted and temporarily stored in lockable bank bags until the funds are safely transferred to the next individual, as defined in the currency chain of custody procedures. Funds used for the purchase of marijuana products will be linked to specific items, lot numbers, and batches within the business management platform and METRC clearly demonstrating the exact products sold, the price of the items, methods of payment, and account details of other medical marijuana organizations where funds

were received or paid.

Receipts of purchases and sales will be made readily available to the CRC and law enforcement officials. Receipts will be observed for their accurate reflection of the transfer of medical marijuana products and funds as part of daily sales and inventory reports.

AGE VERIFICATION AND DISPENSARY ACCESS: STANDARD OPERATING PROCEDURES



Design 710 will refuse to sell cannabis to any person unless the person produces a valid identification showing that the person is 21 years of age or older. N.J.S.A. §17:30-12.3(d) & (e). Identification must be valid and unexpired and contain a photograph and the date of birth of the individual.

Further, we will prominently post notices inside the dispensary that notifies purchasers that minors under age 21 are not permitted on the premises, even in the Mantrap.

Design 710 will require all purchasers to enter the dispensary through the main entrance. Upon arrival to the main entrance vestibule of the facility, also known as the “Mantrap,” a purchaser will check-in with reception, by presenting his or her valid government-issued photo identification to the receptionist via the service window. The receptionist will verify the purchaser’s age and validity of the purchaser’s government-issued identification card by scanning the government-issued identification card with an electronic reader or electronic scanning device. In the instance that two or more purchasers arrive at the same time, they will be instructed to wait in the Mantrap until the receptionist can check them in. After the receptionist has verified the purchaser, he or she will release the locked door from the Mantrap onto the dispensary sales floor. The purchaser will be instructed to wait in a designated waiting area on the floor until he or she is greeted by the next available dispensary sales agent.



Door 1

Door 2

Current Design 710 Medical Dispensary Mantrap: Doors 1 and 2 pictured. All purchasers, visitors, contracted vendors etc. must be buzzed into the security vestibule (Door 1- exterior) to gain access to the facility before ever be allowed to enter (Door 2 – interior photo) into the reception area and adjacent sales floor.

Upon arrival to the main entrance (door 1) vestibule of the facility, a qualifying purchaser will show the Security Officer via the service window his or her valid government-issued photo identification. Once verified as having the appropriate identification, the Security Officer may allow the qualifying purchaser into the facility (door 2) and direct him or her to the reception desk to be checked in. In the instance that two (2) or more qualifying purchasers arrive at the same time, they will be instructed to wait in the main entrance vestibule until verified. Qualifying purchasers will wait in the purchaser waiting area until called to the dispensing sales area. The Mantrap will be fully confined and separated from the Limited Access Area (“LAA”) by a locked door, which will prevent purchasers from entering the LAA without being provided access from a dispensary employee. Once inside the dispensing sales area, a dispensary agent will again verify all purchasers government-issued identification prior to dispensing any cannabis. Specifically, no person will be permitted to purchase any cannabis unless a dispensary agent: (i) verifies the age of the purchaser by checking a government-issued identification card by use of an electronic reader or electronic scanning device to scan a purchaser’s government-issued identification to determine the purchaser’s age and the validity of the identification; (ii) verifies the validity of the government-

issued identification card; and (iii) offers any appropriate purchaser education or support materials. *N.J.S.A. §17:30-12.3(a)*.

AGE VERIFICATION DECLARATIONS

Design 710 affirms that it will strictly adhere to the following declarations:

- Before allowing a consumer to enter its dispensary facility, and prior to selling or serving cannabis items to a consumer, for each transaction, Design 710’s personnel shall examine, authenticate and confirm the legitimacy of photographic identification as defined by the CRC and shall confirm the consumer is of legal age to purchase cannabis (*N.J.C.A. §17:30-12.3(a)*);
- To ensure an individual consumer’s privacy is protected, Design 710 will not require a consumer to provide personal information other than government-issued identification as set forth at *N.J.C.A. §17:30-12.3(a)* above in order to determine the consumer’s identity and age (*N.J.C.A. §17:30-12.3(b)(1)*);
- To ensure an individual consumer’s privacy is protected, Design 710 will not collect and retain any personal information about a consumer other than information typically acquired in a financial transaction conducted by the holder of a Class C retail license concerning alcoholic beverages as set forth at *N.J.S.A. 33:1-12 (N.J.C.A. §17:30-12.3(b)(2))*;
- To ensure an individual consumer’s privacy is protected, Design 710 will not keep a copy of any consumer’s photographic identification (*N.J.C.A. §17:30-12.3(b)(3)*);
- Design 710 will ensure that each and every piece of photographic identification examined from a consumer confirming that consumer’s legal age will be logged in a record and maintained in such a manner that it will be available for inspection by the CRC (*N.J.C.A. §17:30-12.3(c)*);
- In accordance with *N.J.C.A. §17:30-12.3(d)*, Design 710 will not sell to a consumer in a single sales transaction:
 - i. More than one ounce of usable cannabis;
 - ii. The equivalent of more than one ounce of usable cannabis as a cannabis-infused product in solid, liquid, or concentrate form;
 - iii. More than five grams of cannabis concentrate; or
 - iv. Some combination thereof, not to exceed one ounce, or the equivalent, of usable cannabis and cannabis products.

Design 710 will make a good faith effort to prevent a consumer from exceeding one ounce of usable cannabis or the equivalent weight in cannabis products, in multiple sales transactions. *N.J.C.A. §17:30-12.3(e)* by monitoring “repeat visitors.”

AGE VERIFICATION: STANDARD OPERATING PROCEDURES

In an effort to prevent diversion, theft or loss of cannabis, Design 710 will require all purchasers to enter the dispensary through the main entrance. Upon arrival to the main entrance vestibule of the facility, also known as the “Mantrap,” a purchaser will check-in with reception, by presenting his or her valid government-issued photo identification to the receptionist via the service window. The receptionist will verify the purchaser’s age and validity of the purchaser’s government-issued identification card by scanning the government-issued identification card with an electronic reader or electronic scanning device. In the instance that two or more purchasers arrive at the same time, they will be instructed to wait in the Mantrap until the receptionist can check them in. After the receptionist has verified the purchaser, he or she will release the locked door from the Mantrap onto the dispensary sales floor. The purchaser will be instructed to wait in a designated waiting area on the floor until he or she is greeted by the next available dispensary sales agent.

Design 710 will monitor access to the Mantrap and only persons with legitimate reason to be in the Mantrap will be permitted to remain in the Mantrap. As stated above, all purchasers will wait in the Mantrap until allowed into the dispensing sales area. The Mantrap will be fully confined and separated from the limited access area by a locked door, which will prevent purchasers from entering the limited access area without being provided access from a dispensary employee. Once inside the dispensing sales area, a dispensary agent will again verify all purchasers’ government-issued identification prior to dispensing any cannabis. The dispensary agent will also discuss the purchasers product preferences and answer any questions, including by offering any appropriate purchaser education or support materials. Design 710 will refuse to sell cannabis to any person unless the person produces a valid identification showing that the person is 21 years of age or older. N.J.C.A. §17:30-12.3(d) & (e). Identification must be valid and unexpired and contain a photograph and the date of birth of the individual. Further, we will prominently post notices inside the dispensary that notifies purchasers that minors under age 21 are not permitted on the premises, even in the Mantrap.

17:30-12.2 Cannabis retailer authorized conduct; prohibitions....

(d) A cannabis retailer shall not allow persons under the age of 21 to purchase cannabis items or to enter or remain on the premises of a cannabis retailer unless accompanied by a parent or legal guardian and shall ensure similar restrictions are enacted on any internet site operated by the cannabis business.

(e) A cannabis retailer shall not allow persons under the age of 21 to purchase cannabis items.

AGE VERIFICATION: EMPLOYEE TRAINING

Design 710 seeks to create a working environment that leads to high employee retention rates and encourages innovation.

The Human Resources Director and General Manager are responsible for implementation and oversight of employee and contractor training programs. A training schedule is developed and maintained for each position within the Dispensing Organization.



Every employee is initially hired under probationary status. To be released from the probationary status, an employee must complete the following:

- Training: completion of all required training components within three months
- Knowledge: proficiency testing results of no less than 85% on all required exams
- Experience: 80 hours of manager supervised on-the-job training

SOP'S TRAINING

Design 710 is dedicated to training all employees to excel in their position and to properly execute Design 710 SOP's. The SOP system guides agents to follow procedures as written; understand their responsibilities in implementing the SOP's; identify compliance and procedural issues; and report and document all deviations and variances. In addition to New Employee Orientation and other required training, employees must complete ongoing training on SOP's specific to their job tasks, consisting of at least one (1) hour per month. Once authorized to perform the task, the employee must have a digital or print version of the most current SOP in front of them each time they perform the task to ensure no step is missed. Current versions of SOP's will always be available online and in print so employees can easily refer to them. Annual assessments will be conducted to re-certify the employee in each task.

Specific training on key topics in the SOP's is further addressed in the two following sections, Training On Rules and Laws to be Followed and Training on Safely Using Cannabis/Dispensary Products and Other Topics.

POINT OF SALE TRAINING

Effectively operating the point-of-sale system and the state's verification system; Proper inventory handling and tracking; Regulatory inspection preparedness and law enforcement interaction.

The General Manager will train all employees directly involved in dispensing of cannabis products on the following topics:

- Point of sale and verification operations, including using METRC, New Jersey's Official State Cannabis Traceability System.
- Dispensing and reporting legal requirements.
- Qualifications for the sale of cannabis, including age verification and ID-verification and documentation in N.J.C.A. 17:30-12.3(a).
- Daily purchasing limits and the legal possession limit defined as defined by law;
- Superior customer service skills.



Pursuant to N.J.C.A. 17:30-3.6 and 9.6(a)(1)(v) and 9.13 (“Inventory Control System”), Design 710 will train employees to document and record every transaction, sale, and transfer. Design 710 will also train employees how to maintain those records and make them available to the Regulators.

QUALIFICATIONS FOR SALE TRAINING

Effectively operating the point-of-sale system and the State’s verification system

To prevent diversion and maintain regulatory compliance, Design 710’s employees will be trained to only sell cannabis when the following conditions are met:

- Employee is able to verify the identity and age of the purchaser via a valid driver license or other government-issued photo ID, including acceptable forms of identification, N.J.C.A. §17:30-12.3(a);
- Employee is able to verify the validity of the ID, by using an electronic reader or scanner, N.J.C.A. §17:30-12.3(a);
- The cannabis product being sold or transferred has been tested and is packed and labeled in accordance with and any additional rules set out by the CRC. N.J.C.A. §17:30-13.



Employees will receive thorough training on how to check identification and common mistakes made in the verification process. Employees will also have access to state of the art ID verification technology devices that are used in bars, nightclubs, member clubs, any business checking the age of their customers and require an ID Scanning.

PURCHASE LIMIT TRAINING

Effectively operating the point-of-sale system and the state’s verification system;

Proper inventory handling and tracking. Design 710’s employees will be trained to strictly adhere to purchasing limits, as set forth in N.J.C.A. §17:30-12.3(d), and will not sell to a consumer in a single sales transaction:

- v. More than one ounce of usable cannabis;
- vi. The equivalent of more than one ounce of usable cannabis as a cannabis-infused product in solid, liquid, or concentrate form;
- vii. More than five grams of cannabis concentrate; or
- viii. Some combination thereof, not to exceed one ounce, or the equivalent, of usable cannabis and cannabis products.

Violation of this SOP will result in immediate termination of the employee. The General Manager will log the incident and notify the CRC. By ensuring mandatory possession limits are maintained, Design 710 will enhance its security efforts, maintain the safety of its host community and the purchaser, and otherwise ensure the integrity of the program is maintained.

Standard Operating Procedures (“SOPs”) for Dispensing



All cannabis products will be tracked and monitored in METRC and by Design 710’s physical inventory audits under §17:30-12.8(k), 9.7, and 9.13. METRC will create a timestamp, which will be used to produce a receipt that may be printed and made available to the CRC, law enforcement, and company management. Design 710’s Dispensing SOPs comply with §17:30 and other applicable requirements and cover a multitude of operations including measures

to ensure non-diversion of cannabis products and materials, including fidelity to product tracking best practices, rigorous age verification practices, and standards to avoid “straw” purchasing for minors (including adherence to quantity limits that may be purchased by each customer). Additionally, Design 710’s delivery and transport SOP’s include:

- Taking orders, verifying photographic identification and taking payment;
- Logging the transactions in METRC and, as applicable, internal inventory;
- Conducting in-person deliveries, which shall include protocols for use of personal protective equipment and regular sanitization if necessary to prevent spread of diseases such as COVID-19;
- Maintaining privacy and confidentiality of the purchasing consumer’s purchase information;
- Training cannabis business delivery personnel;
- Security for cannabis business delivery personnel, delivery vehicles and inventory; and
- Emergency notification and response in the event of accidents, theft, equipment malfunction, or other emergency events.

Delivery	Sales	Patient	Driver	Vehicle Info	ETD	ETA	AA	Completed	Total	Recorded	State
0000000142	09/03/2020 04:11 pm	134303447	Joseph Johnson	Make: Toyota Model: Tacoma Lic Plate: RC2080428	09/03/2020 04:21 pm	09/03/2020 04:41 pm		\$25.00	09/03/2020 04:13 pm	Shipped	
0000000016	09/03/2020 03:38 pm	134303447	Joseph Johnson	Make: Toyota Model: Tacoma Lic Plate: RC2080428	09/03/2020 03:38 pm	09/03/2020 03:58 pm		\$1.00	09/03/2020 03:38 pm	Completed	
0000000017	07/06/2020 11:15 am	12345	Joseph Johnson	Make: Toyota Model: Tacoma Lic Plate: RC2080428	07/06/2020 11:15 am	07/06/2020 11:29 am		\$10.00	07/06/2020 10:17 am	Completed	
0000000018	09/03/2020 09:28 pm	134303447	Joseph Johnson	Make: Toyota Model: Tacoma Lic Plate: RC2080428	09/03/2020 09:28 pm	09/03/2020 09:48 pm		\$10.00	09/03/2020 09:27 am	Completed	
0000000019	04/14/2020 12:13 pm	12345	Joseph Johnson	Make: Toyota Model: Tacoma Lic Plate: RC2080428	04/14/2020 12:13 pm	04/14/2020 12:13 pm		\$50.00	04/14/2020 10:14 am	Completed	
0000000020	03/07/2020 09:43 pm	134303447	Joseph Johnson	Make: Toyota Model: Tacoma Lic Plate: RC2080428	03/07/2020 09:43 pm	03/07/2020 09:43 pm		\$20.00	03/07/2020 09:43 pm	Completed	

On-Site Age Verification



Design 710 has developed comprehensive procedures to ensure no person under the age of 21 will be permitted to purchase any cannabis or cannabis products. §17:30-12.2(e). No person under the age of 21 will be permitted to enter the facility unless accompanied by a parent or legal guardian. §17:30-12.2(d). All persons entering the facility must present acceptable photographic identification. The identification must not be ripped, torn, punched, bleeding print, pixilated images, or have proper lamination. Without acceptable photographic identification, they will be asked to leave. Design 710 procedures detail acceptable forms of identification,

including: (1) any countries passport or proper government-issued document for international travel, provided it is lawful to use as identification in the United States (§17:30-12.3(a)(1)); (2) A motor vehicle driver’s license issued by any state, territory, or possession of the United States of the District of Columbia, provided the license displays a picture of the person (§17:30-12.3(a)(2)); (3) A New Jersey Identification Card issued by the New Jersey Motor Vehicle Commission (§17:30-12.3(a)(3)); or, (4) Any other identification card issued by a state, territory, or possession of the United States, the District of Columbia, or the United States that bears a picture of the person, the person’s date of birth, and a physical description of the person. §17:30-12.3(a)(4).

Consumer Data Privacy

Design 710 training materials pay specific attention to the limitations of collecting personal data. No personal information other than the government-issued identification set forth above will be utilized to determine the consumer’s identity and age. §17:30-12.3(b)(1). In accordance with §17:30-12.3(b)(2), no personal information of the consumer will be collected or retained in this

electronic log other than as acquired in a financial transaction mirroring the information collected by a Class C retail license holder for alcoholic beverages under N.J.S.A. 33:1-12. A copy of the consumer's photographic identification will NOT be created or retained. §17:30-12.3(b)(3). Instead, Design 710's personnel will log that the examination of the photographic identification and confirmation of age occurred and will make said log available to the CRC for inspection upon request §17:30-12.3(c).

Age Verification in Marketing

No individual under the age of twenty-one ("21") will be permitted to enter Design 710's internet site. §17:30-12.2(d). Individuals accessing Design 710's website will be subject to an age verification system as a technical protection measure to restrict the access of those under twenty-one. To prevent unauthorized access by individuals under twenty-one, consumers will be initially presented to a notice page that refuses entry to those under 21. Visitors will then be required to input their date of birth and affirm the veracity of their inputs. Should the visitor order cannabis or cannabis products on Design 710's website, their identification will be verified in person either at our facility or prior to completing delivery consistent with the preceding paragraph above. Using these procedures, Design 710 will ensure that underage individuals are not provided cannabis or cannabis products in clear contradiction of the law.