Summit Wellness, LLC

Security Plan

Introduction

Summit Wellness, LLC (Summit Wellness) will meet all security requirements in accordance with the New Jersey Cannabis Regulatory, Enforcement Assistance, and Marketplace Modernization Act (N.J.S.A. 24:6I-31, et seq.) and its implementing regulations at N.J.A.C. 17:30-1.1, et seq., as well as any local security requirements mandated by Jersey City. 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.

Summit Wellness shall provide effective controls and procedures to guard against unauthorized access to the premises or the business' electronic systems, theft, and diversion of cannabis. These controls are discussed in more detail below:

1. 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. Our staff will be trained on Summit Wellness security procedures and agents will be thoroughly familiar with a range of security topics, including anti-diversion; physical safety; suspicious activity reporting; evacuation; fire; theft; and emergency communications, among other topics. The plan will be presented to all employees and used as the basis for detailed instructions in building security measures, personnel security measures, emergency response procedures, daily normal checklists, and emergency contact procedures.

1.1 Key responsibilities of the Security Manager:

1.1.1 Ensuring that only individuals aged 21 years or older, unless accompanied by a parent or legal guardian, are permitted access to the premises, in accordance with N.J.A.C. 17:30-12.2(d).

1.1.2 Ensuring that only individuals aged 21 or older are permitted to purchase cannabis items, in accordance with N.J.A.C. 17:30-12.2(e).

1.1.3 The safety of customers, staff, and visitors to the facility.

1.1.4 The training of staff in all security-related procedures.

1.1.5 The prevention of diversion.

1.1.6 The safe and secure storage of inventory.

1.1.7 The integrity of perimeter and facility security.

1.1.8 Ensuring that all security systems and technologies function correctly, meet legal and code requirements, and are regularly maintained to prevent failure and ensure compliance.

1.1.9 The enforcement of all security-related matters.

2. 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, in accordance with N.J.A.C. 17:30-9.10(b)5.

2.1 Alarms

2.1.1 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.

2.1.2 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 should this be needed.

2.1.3 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.

2.1.4 Control panels for the alarm systems will be located in a closed cabinet by the main entrance to the retail store.

2.1.5 The alarm systems will also include the following functionality:

- 2.1.5.1 Battery backup or generator for the system in the event of power outage.
- 2.1.5.2 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.
- 2.1.5.3 Silent mode to protect employees if perpetrators are armed or in case of ambush.
- 2.1.5.4 Duress and Panic alarms
- 2.1.5.5 Visual and/or audible alert (flashing lights and sirens on the exterior of the building to notify passing police a robbery is in progress).
- 2.1.5.6 Cell phone back-up in event telephone or internet connection is cut.

2.1.6 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.

2.1.7 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.

2.1.8 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. Summit Wellness will be notified by our monitoring company of any loss of power within 5 minutes of the event. We will then activate the on-site generator until full power to the facility is restored. All of these mitigation techniques meet, and in most cases exceed the Nj Cannabis Regulatory Commission (CRC) requirements to remain in compliance during a power outage.

2.2 Video Surveillance

2.2.1 The surveillance system will be recording 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.

2.2.2 The server, control system, telecommunications system, and backup power generator 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 CRC. A current list of authorized employees and service personnel that have access to the surveillance room must be available to the CRC upon request.

2.2.3 Critical areas—internal:

2.2.3.1 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.

2.2.4 Critical areas—external:

2.2.4.1 the full perimeter of the facility, all entrances, the parking lot, and parking lot entrance.

2.2.5 Trees bushes and other vegetation will be regularly trimmed and maintained to ensure full visibility and deny opportunities for concealment.

2.2.6 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.

2.2.7 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.

2.2.8 All video recordings from all cameras must, upon request, be made available for immediate viewing by the CRC.

2.2.9 All video recordings must be retained for at least 90 calendar days.

2.2.10 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.

2.3 Recording Standards

2.3.1 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. All video recordings will be maintained for 90 days, far exceeding the standard set by the CRC. All recordings will be backed-up and retained on record for no less than 90 days via external hard drive and cloud storage, and shall be immediately available upon request by the CRC or Law Enforcement.

2.3.2 The system will have the capability of immediately producing a clear, color, still photo whether live, or recorded. 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. A suitably trained member of staff will be available during hours of operation to facilitate the viewing of surveillance footage and provide still photos where appropriate.

2.3.3 All recordings must be erased or destroyed prior to disposal.

2.3.4 The video and recording system will be equipped with a battery back-up or generator for the system in the event of power outage.

3. Access Control

3.1 Retail Facility

3.1.1 When closed for business the facility will be closed and secured in accordance with the closing procedures outlined below.

3.1.2 When opening for business the facility will be opened in accordance with the opening procedures outlined below.

3.1.3 All employees of the facility will visibly display an employee identification badge issued by the company at all times while at the retail facility.

3.1.4 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 cannabis 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 CRC at all times.

3.1.5 All employees will be issued with an electronic “swipe” card that affords them access to certain rooms and spaces within the facility.

3.1.6 These cards track the time and individual gaining access to the various restricted areas.

3.1.7 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.

3.1.8 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.

3.1.9 In accordance with N.J.A.C. 17:30-12.7, only an owner, principal, employee, or volunteer of Summit Wellness that possesses a Cannabis Business Registration Card when acting in their official capacity shall have access to the enclosed, indoor, locked area storing cannabis items per N.J.A.C. 17:30-9.12.

3.1.10 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.

3.2 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.**

3.3 Access Levels

3.3.1 **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.

3.3.2 **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.

3.3.3 **Owners and Investors** – Will NOT be provided with any key, “swipe” card, code or combination unless they are a cannabis business identification card holder 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).

3.3.4 **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 logbook provided. All visitors are to be accompanied by an escort with a Cannabis Business Identification Card ALL times. Summit Wellness will retain the visitor log for a one-year period. For the avoidance of confusion, a "Visitor" is an individual visiting the facility for a purpose other than purchasing products and therefore, a "Visitor" is not considered a "customer".

3.3.5 **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 logbook provided. All contractors are to be accompanied by an escort with a Cannabis Business Identification Card at ALL times.

3.3.6 **Deliveries** - Only designated agents of Summit Wellness will transport cannabis or cannabis products, during the course of business operations. Summit Wellness may also contract with a legal Third-Party Transporter duly licensed by the Cannabis Control use a licensed cannabis distributor for such transport. Records of all deliveries of cannabis to Summit Wellness will comply with all CRC regulations, and will contain the following information:

3.3.6.1 The date and time that the transport began and ended;

3.3.6.2 The name, Cannabis Business Identification Card number, and signature of the cannabis business staff member performing the transport;

3.3.6.3 The weight of the cannabis or cannabis item transported;

3.3.6.4 The batch number of the usable cannabis or the lot number of the cannabis product, the name of the strain/cultivar, and the form of the cannabis product; and

3.3.6.5 the signature of the cannabis business staff member of the receiving cannabis business attesting to the receipt of goods.

3.4 Lost/Stolen Card/Key Procedures

3.4.1 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:

3.4.1.1 The store manager must be notified in person **IMMEDIATELY** when 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.**

3.4.1.2 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.

3.4.1.3 The holder of the lost card should notify the manager when, where, and how they believe the card was lost.

3.4.1.4 The store manager (or duty manager) must immediately access the system and cancel the "swipe" card in question.

3.4.1.5 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 CRC informed.

3.4.1.6 A new card may only be issued upon completion of the above steps.

3.4.1.7 Loss of a replacement card may be grounds for dismissal.

3.4.2 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:

3.4.2.1 A senior manager must be notified in person **IMMEDIATELY** when 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.**

3.4.2.2 In the event the senior manager cannot be reached, the store manager must be informed on the same terms as above.

3.4.2.3 The holder of the lost key should notify the senior manager when, where, and how they believe the key was lost.

3.4.2.4 The senior manager or store manager must immediately attend the store with their personal set of building access keys.

3.4.2.5 A locksmith will be called and all compromised locks will be changed immediately.

3.4.2.6 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 CRC informed.

3.4.2.7 The senior manager will supervise the recall and replacement of all building access keys.

3.4.3 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:

3.4.3.1 The duty store manager must be notified in person **IMMEDIATELY** the loss is identified.

3.4.3.2 The custodian of the lost key(s) should notify the duty store manager when, where, and how they believe the key(s) was lost.

3.4.3.3 The store manager will immediately lock the secure storage area using, if necessary, the reserve key kept in the safe.

3.4.3.4 A locksmith will be called, and all compromised locks will be changed immediately.

3.4.3.5 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 CRC informed.

3.4.3.6 A senior manager will supervise the recall and replacement of all secure storage keys.

3.5 Locks, Cabinets, and Safes

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.

Cash Vault – An on-site, locked safe or vault maintained in the secure storage area and used exclusively for the purpose of securing cash; Video cameras directed to provide images of areas where cash is kept, handled and packaged for transport to financial institutions or DOR facilities. Further, that all cameras be able to produce a clear, still image whether live or recorded;

3.5.1 **Keys:**

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

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

3.5.2 **Codes:**

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

3.5.2.2 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.

3.5.2.3 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.

3.5.2.4 Codes may not be written down, noted, recorded, texted, or e-mailed to any individual at any time.

3.5.3 **Combinations:**

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

3.5.3.2 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.

3.5.3.3 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.

3.5.3.4 Combinations may not be written down, noted, recorded, texted, or e-mailed to any individual at any time

3.5.4 **Changes to codes and combinations:**

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

3.5.4.2 Senior Management will be responsible for the scheduling and change of such codes and combinations.

3.5.4.3 All changes to codes and combinations will be provided to authorized recipients **IN PERSON**.

3.5.4.4 Codes and combinations may not be written down, noted, recorded, texted, transmitted or e-mailed to any individual at any time.

3.5.4.5 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.

4. Incident Reporting

In accordance with N.J.A.C. 17:30-9.10, Summit Wellness’ safety and security alarm system will provide immediate automatic or electronic notification to alert cannabis business personnel and State or local police agencies to an unauthorized breach of security or an alarm or system failure at the cannabis business.

4.1 List of Incidents Requiring Reporting (non-comprehensive)

4.1.1 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.

4.1.2 When a qualified person pursuant to N.J.A.C. 17:30-8.1(a) ceases to work at or be affiliated with Summit Wellness (10 days – N.J.A.C. 17:30-8.2).
4.1.3 Loss, discrepancies identified during inventory, diversion or theft, whether or not the cannabis, funds, or other lost or stolen property is subsequently recovered and/or the responsible parties are identified, and action taken against them (immediately to law enforcement, 3 hours to CRC – N.J.A.C. 17:30-9.11(a)).
4.1.4 An alarm activation or other event that requires response by public safety personnel (24 hours – N.J.A.C. 17:30-9.11(b)).
4.1.5 A breach of security (24 hours – N.J.A.C. 17:30-9.11(b)).
4.1.6 Corrective measures taken, if any (24 hours – N.J.A.C. 17:30-9.11(b)).
4.1.7 The amount of cannabis destroyed, including the form, weight, quantity, and any other information requested by the CRC (24 hours – N.J.A.C. 17:30-9.11(b)).

All documentation related to an incident that is reportable will be retained by Summit Wellness, for not less than two years or the duration of an open investigation, whichever is longer, and made available to the CRC and law enforcement authorities upon request.

5. 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 cannabis products.

5.1 General

5.1.1 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.
5.1.2 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.
5.1.3 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.
5.1.4 Each visitor must present official or state-approved photo-ID, and sign our logbook, 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.
5.1.5 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.
5.1.6 Retail store employees must ensure that all cannabis inventory remains in locked storage which is accessible only to other authorized members of staff.
5.1.7 Each retail store employee must summon a supervisor to count 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.
5.1.8 Retail store employees will check all locks, alarms, cameras and security equipment before leaving for the night.
5.1.9 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.

5.2 Required General Functions for Security Agents

5.2.1 At least one Security Agent that is a State Certified Security Officer whose certification is in good standing shall remain on-site during operating hours.

5.2.2 Prohibit the formation of a queue outside the building.

5.2.3 Monitor and enforce Occupancy Limit. Should the Occupancy Limit be reached, new customers will be asked to order the product they seek online and come back to pick up the product at a later time.

5.2.4 Refuse entry to any customer who parks illegally on Alliance Street.

5.2.5 Ensuring that there is no on-site consumption of cannabis products. To that end, a Security Agent shall survey the parking lot on an hourly basis to ensure that no one is consuming cannabis on the premises. If consumption is occurring, the person will be notified by the Security Ageny that consumption on the premises is prohibited. If the person refuses to stop consuming, the police department will be contacted.

5.2.6 Assist employees and visitors in the facility as well as assist with deliveries. This may include general assistance in matters not directly related to security (directions, program information, etc.)

5.2.7 Provide or assign employee escorts to visitors as required.

5.2.8 Monitor and control access to the Summit Wellness facility to only those authorized individuals.

5.2.9 Monitor surveillance cameras to observe any suspicious person or behaviors both within and outside the property.

5.2.10 Locate lost or stolen property.

5.2.11 Constantly be aware of your surroundings, ask questions and be engaged with individuals in a courteous manner.

5.2.12 Use de-escalation techniques on individuals whose goal is to harm individuals inside or outside of the facility.

5.2.13 Protect persons and property against attempts to commit crimes of various natures by reporting suspicious incidents and behaviors promptly to local law enforcement.

5.2.14 Immediately contact local law enforcement and report any violent or hostile behavior by subjects inside or outside the facility.

5.2.15 Render first aid in warranted situations.

5.2.16 Our security agents will not be armed, and their primary equipment will include a cell phone, walkie talkie radio, and a mobile point-of-sale device to monitor Occupancy Limit.

5.3 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**

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

5.3.1 In the event of an armed hold-up, comply with all demands in a polite, courteous and efficient manner.

5.3.2 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.

5.3.3 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 without being noticed, then do so with **extreme caution**.

5.3.4 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**.

5.3.5 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.

5.3.6 If possible, tell the employees that they are to do everything the perpetrator asks.

5.3.7 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.

5.3.8 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.

5.3.9 If the robber demands the inventory, show them where sales stock is kept on the retail floor (securely locked in the sales cabinet), but do not point out the secure storage room unless they demand to know. Open the locked cabinet for them, and back away.

5.3.10 While the robbery is in progress, employees should make note of their physical characteristics:

5.3.10.1 Approximate height and weight, any sort of accent, distinguishing features such as scars or tattoos

5.3.10.2 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?

5.3.10.3 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?

5.3.10.4 Did they touch anything with an ungloved hand or commit any act that may have left DNA evidence behind (spitting, drinking, smoking)?

5.3.11 **Any other potential evidence should be left untouched and protected from tampering until police arrive.**

5.3.12 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.

After the Robbery

5.3.13 The police should be contacted as quickly as possible using any means necessary.

5.3.14 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.**

5.3.15 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 until the EMTs arrive.

5.3.16 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.

5.3.17 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.

5.4 Fire in the Facility

Summit Wellness has developed the following fire emergency plan that will be taught practiced by all employees for implementation in the event of a fire on the premises.

5.4.1 In the event of noticing smoke or a fire, activate the fire alarm and announce that the building needs to be evacuated.

5.4.2 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.**

5.4.3 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.

5.4.4 Once outside, The Store Manager should verify that all members of staff are present.

5.4.5 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.

5.4.6 Make sure the entrance to the facility is unobstructed allowing access for fire department vehicles. No one should ever be parked in front of the facility. However, ask anyone present who has parked in front of the facility to please move their vehicle immediately to facilitate access for the emergency services.

5.4.7 When the fire department arrive, detail where you believe the fire started, and where it is the most intense.

5.4.8 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 ensure 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.

6 Store Opening Procedures

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

6.1 General Order of Opening (non-comprehensive; security procedures only)

- 6.1.1 Manager or keyholder and one other member of staff should arrive 30 minutes prior to store opening to insure readiness.
- 6.1.2 Under no circumstances should the manager or keyholder open or enter the facility alone.
- 6.1.3 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.
- 6.1.4 Unlock and enter the building. Ensure that no error or activation codes are present on the alarm system.
  - 6.1.4.1 **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.**
- 6.1.5 Disarm 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.
- 6.1.6 Turn on lights for store operations.
- 6.1.7 Perform a visual check to ensure all windows, inventory, and physical assets are undisturbed.
- 6.1.8 Open the secure storage room only to facilitate the processing of sales stock.
  - 6.1.8.1 **The secure storage room is to remain locked at all times**, except when certain activities necessitate its opening.

7 Store Closing Procedures

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.

7.1 General Order of Closing

- 7.1.1 Do not extinguish or dim any lights until all customers have left the facility.
- 7.1.2 Do not close the registers until after the scheduled closing and ensure all customers have exited the store. Check all restrooms to ensure there is no one left but employees.
- 7.1.3 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.
- 7.1.4 Check the phone for any unanswered voicemail.

7.1.5 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.
7.1.6 Place trash bags at door for removal and disposal upon exit.
7.1.7 Look outside and ensure that the store exit safety lights are on.
7.1.8 Lock all perimeter doors including the main entrance and any exit doors.
7.1.9 Count cash in the secure storage room.
7.1.9.1 All counting and cash-related closing activities must be completed in the designated area of the secure storage room so as to remain in view of cameras.
7.1.9.2 Counting should never be done in view of windows or customers.
7.1.10 Complete inventory reconciliation reports.
7.1.11 The manager should perform a bag/coat check of exiting employees.
7.1.12 Activate alarm system, turn off all lights, exit and secure the premises.
7.1.13 Walk around the outside of the building and make a final check that all doors, windows and points of entry are secured.

8 Inventory Control and Reconciliation

In accordance with N.J.A.C. 17:30-9.12(b) all cannabis 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 cannabis products arrive pre-packaged from our supplier's facility, where it has been weighed, packaged, labelled and bar-coded. cannabis 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 following procedures will be included in the cannabis business operations manual in accordance with N.J.A.C. 17:30-9.6.

8.1.1 The store manager, in their role as security manager is responsible for opening the container and matching the manifest to products contained within.
8.1.2 The label must indicate the originating cannabis establishment name, address and registration name.
8.1.3 The store manager must note and record the name and registration number of the agent who prepared the manifest.
8.1.4 The store manager should check each item and identify any that are outdated, damaged, mislabeled, contaminated or compromised. Any such products should be set aside for disposal.
8.1.5 The store manager must carry out this process in the presence of at least one other cannabis business license holder.
8.1.6 All products must be scanned, weighed, and immediately entered into the retail store inventory.
8.1.7 Any discrepancies must be **immediately** reported to Senior Management and documented.
8.1.8 The container may only be opened in a designated secure area.
8.1.9 The entire delivery arrival and unpacking process must be recorded on surveillance or video cameras to ensure the integrity of the chain of custody.
8.1.10 The store manager signs the manifest and enters the new inventory into the "Metrc seed-to-sale" tracking software.
8.1.11 The store manager stores all new inventory in its appropriate place in the vault and places the original manifest in the safe.

8.1.12 Inventory is to be generally stored in the secure storage room. Sufficient sales stock for each days' business will be removed from the vault and securely stored on the retail 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 retail floor.

8.1.13 The vault door must be kept locked at all times and may only be opened to perform necessary tasks before being locked once more.

8.1.14 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.

8.1.15 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 cannabis products have been moved from the active database to the "dead" inventory file.

8.1.16 When finished, the store manager must save the reconciliation report using the "Metrc seed-to-sale" tracking software. Variances between expected inventory and actual inventory must be **immediately** reported to Senior Management and documented.

8.1.17 These reports are checked each day by our internal auditor. Unreported discrepancies will be flagged, documented and **immediately** exported to Senior Management.

8.1.18 Each and every discrepancy will be personally investigated by Senior Management, or their deputy, within 24 hours.

8.1.19 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.

8.1.20 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.

8.1.21 In the event the inventory was taken by a store employee they will be terminated, and the police will be notified for possible prosecution.

8.1.22 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.

9 Storage of Cannabis

9.1.1 In accordance with N.J.A.C. 17:30-12.7, all cannabis products will be stored in an enclosed indoor, locked area where access to such area is limited to an owner, principal, employee, or volunteer of Summit Wellness that possesses a Cannabis business Identification Card when acting in their official capacity.

9.1.2 All cannabis and cannabis products will be securely stored in the security vault at all times when the facility is closed for business or unattended.

9.1.3 The security vault will be alarmed and secured with a U.L. group 1 combination lock and is sited in an area away from public view.

9.1.4 The security vault will contain a separate area for the storage for disposal of products that may be outdated, damaged, deteriorated, compromised, mislabeled, or whose containers or packaging have been opened or breached.

9.1.5 The security vault will be maintained in a clean and orderly condition and will be free from pest infestation of any kind.

9.1.6 At the beginning of each business day the store manager, together with their staff, will remove from the vault only those products needed for the day ahead. The products removed will be noted on an inventory sheet. All other products must remain in the vault which should be kept locked at all times.

9.1.7 Products brought onto the sales floor in this manner must be placed and secured inside the display cabinets and only removed for sales purposes.

9.1.8 Should it become necessary for the store manager to open the vault to retrieve additional items during the course of the working day, the required items should be removed from the vault, entered onto the inventory sheet and the vault locked again in a timely fashion.

9.1.9 At the end of each working day, products from the shop floor will be tallied against the inventory sheet and returned to the security vault for overnight storage.

10Quality Control and Testing

All of our products are sold pre-packaged and tested by our cultivation and manufacturing suppliers. The initial quality control and testing of these products is the responsibility of these suppliers. That being said, there are certain steps that we can take to ensure that the products entering our inventory are tested, have achieved the correct quality, and are stored and rotated in a manner the best ensures their continued quality throughout their shelf-life.

10.1.1 All products must be thoroughly checked upon arrival at our facility in accordance with **Transportation of cannabis** and **Inventory Control and Reconciliation** protocols above.

10.1.2 The store manager should check each item and identify any that are outdated, damaged, mislabeled, contaminated or compromised. Any such products should be set aside for disposal.

10.1.3 Once the products enter our inventory it is the store manager’s responsibility to ensure that:

10.1.3.1 Stock is efficiently rotated to ensure that older product is sold before newer product.

10.1.3.2 All stock is appropriately stored to prevent spoiling and damage to the product.

11Prevention of Diversion and Theft

11.1.1 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.

11.1.2 Our surveillance system is capable of recording all activities, 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.

11.1.3 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 video recordings and inventory counts and determine the correct course of action.

11.1.4 Whenever inventory is stolen, the police, the CRC 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.

12Waste 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 cannabis products by their removal with trash for later retrieval we have developed the following procedures. In the course of normal operations small amounts of cannabis waste may be generated from (for example) broken packaging, or customer returns. All cannabis waste must be disposed of in accordance with N.J.A.C. 17:30-9.14.

12.1 Regular Waste Disposal Procedures

12.1.1 During the shift, all waste is to be placed in the storage container in the work room.

12.1.2 The manager will help put the stored waste into disposal bags, ensuring that no inventory is included with the waste.

12.1.3 During closing procedures (see above), the manager will bring the bag of waste outside to the dumpster.

12.2 Cannabis Waste Disposal Procedures

12.2.1 All cannabis waste must 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.

12.2.2 All waste must be held for seven (7) days.

12.2.3 At the end of the seven days the cannabis waste will be ground and mixed with other organic waste in a manner that renders the cannabis unusable for its original purpose and deposited at the local landfill.

12.2.4 At least two Summit Wellness employees must witness and document this process.

12.2.5 Within 10 business days after destroying the cannabis, Summit Wellness shall notify the CRC, in writing, of the amount of cannabis destroyed, including the form, weight, quantity, and any other information requested by the CRC.

13Information 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 CRC requirements.

13.1 Primary Software Systems

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

13.2 Primary Hardware Systems

13.2.1 Security system
13.2.2 Point of Sale system
13.2.3 Scanners, card, and barcode readers
13.2.4 Printers
13.2.5 Modems and routers
13.2.6 Local area network
13.2.7 Workstation computers
13.2.8 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.

Summit Wellness, its employees, 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.

13.3 Acknowledgement

13.3.1 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 Summit Wellness.
13.3.2 Acknowledgement is required at the time of initial employment and annually thereafter.
13.3.3 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.
13.3.4 Those employees whose job responsibilities require them to access credit card information will be required to participate in annual security awareness training.

13.4 Employee Administration

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

13.4.2 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.

13.4.3 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.

13.5 Contractors and Temporary Workers

13.5.1 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.

13.6 Acceptable Use

13.6.1 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.

13.6.2 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 company computing environment. If users have any uncertainty on the appropriateness of their actions, they should clarify their understanding with their manager.

13.7 Equipment and Media Security

13.7.1 Lost or stolen electronic devices must be reported to senior management immediately. This includes laptops, smartphones, or removable storage devices that contain company data.

13.7.2 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.

13.7.3 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.

13.8 Security Controls

13.8.1 Senior management oversees the infrastructure and controls for centralized networks, servers, databases and desktop computers.

13.8.2 Users must not disable, uninstall, or modify the security software, settings or encryption installed on laptops or mobile devices.

13.9 Security Logging and Monitoring

13.9.1 Logs of key system events and access to sensitive information are in place and administered by senior management.

13.9.2 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.

13.9.3 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.

13.9.4 Logs are protected from unauthorized modification or destruction and are retained for a minimum of 180 days or as required.

13.9.5 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.

13.10 Third Party Access

13.10.1 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.

13.10.2 Vendors or other third parties with access to the company-owned or leased equipment or systems housed in the company data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

13.11 Access Control

13.11.1 Access to the company systems and applications is role-based and will be granted to authorized users based on job classification.

13.11.2 Users are limited to the system capabilities they need based on job function or role and as authorized by management.

13.11.3 The company computers are equipped with screensaver locks that will activate after 15 minutes of inactivity.

13.11.4 Users must manually log off or lock workstations if they will be unattended prior to activation of the screensaver lock.

13.12 System and User Accounts

13.12.1 Accounts are assigned to an individual and may not be shared.

13.12.2 Guest accounts must be disabled if a system or application is provided with one.

13.12.3 Vendor-supplied default accounts and passwords must be disabled or changed.

13.12.4 System accounts, such as background accounts that are used for internal processing, are exempt from time-based password change requirements.

13.13 Passwords

13.13.1 Passwords are confidential and must not be shared.

13.13.2 Passwords must be changed on first use or if they have been reset for the user by senior management.

13.13.3 Senior management and other administrators resetting passwords must verify the identity of all users requesting a password reset prior to performing the reset.

13.13.4 The primary user password must be changed at least every 90 days.

13.13.5 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.

13.14 Account Review

13.14.1 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.

13.14.2 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.

13.15 Network Connectivity

13.15.1 All devices should primarily access the internet through our LAN. Wi-Fi use will be restricted certain limited devices only.

13.15.2 Senior management oversees the company's network, and all new wired connections must be requested through them.

13.15.3 Wired devices, such as servers, that will be connected to the network must be approved and implemented by senior management for their respective networks.

13.15.4 Employees and other authorized users must request remote access and use established connectivity methods to connect to the company networks from a remote location.

13.15.5 Use of other remote connectivity methods is prohibited.

13.16 Changes to Applications

13.16.1 Application change control is a security issue because unauthorized or accidental changes to applications may impact the integrity and availability of the data.

13.16.2 The ability to change applications is limited to authorized users.

13.16.3 Applications managed by senior management may not be changed without their permission.

13.16.4 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.

13.17 Security Incident Response

13.17.1 All users must report suspicious activities or actual occurrence of any unauthorized activities to the store manager who must, in turn, notify senior management.

13.17.2 Notification should be made immediately or as soon as reasonably possible to senior management and/or law enforcement. 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.

13.17.3 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.

13.17.4 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.

13.17.5 Users detecting potential information security events should immediately report them to the store manager.

13.18 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.

13.19 Backups

13.19.1 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 personal devices. If additional storage space is needed, contact your supervisor for options.

13.20 Compliance and Audit

13.20.1 **Compliance with Legal Requirements:**

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

13.20.2 **Third-Party Service Providers:**

13.20.2.1 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:

13.20.2.2 Take reasonable steps to confirm that the service provider is

13.20.2.3 capable of maintaining appropriate security measures to protect personally identifiable information consistent with all applicable laws and regulations, and;

13.20.2.4 Require the service provider to contractually agree in writing with the company to implement and maintain such appropriate security measures.

13.20.3 **Audit:**

13.20.3.1 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.

13.21 Enforcement

13.21.1 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 Summit Wellness.

13.22 Exceptions

13.22.1 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.