COACHILLIN'

INDUSTRIAL CULTIVATION & ANCILLARY CANNA-BUSINESS PARK

PROJECT SECURITY PLAN

UPDATED August 2017

VETERANS HIGH RISK SECURITY SOLUTIONS

PRIVATE SECURITY

Applicant: Coachillin' Holdings LLC
Project Title: **COACHILLIN' INDUSTRIAL CULTIVATION & ANCILLARY CANNA-BUSINESS PARK**
Project Location: NEC of Indian Canyon Drive between 18th Avenue and 19th Avenue,
City of Desert Hot Springs, California 92240

DATE: August 21, 2017

TABLE OF CONTENTS

COACHILLIN' INDUSTRIAL CULTIVATION & ANCILLARY CANNA-BUSINESS PARK

***Disclaimer**: All canna-business operators within the Coachillin Park are independently owned and operated. COACHILLIN HOLDINGS LLC (CHL) is strictly ancillary to the cannabis industry. Neither Coachillin Holdings LLC nor any of it Members operate, or control cannabis business facilities of any kind (cultivation, extraction, or other); Coachillin Holdings is simply ancillary in its ownership of buildings that CHL develops for sale and/or lease within the project (i.e. Coachillin Holdings is a developer / landlord only). For the purposes of this document, references to "COACHILLIN'" is intentded to convey the project as a whole, and should not be interpreted to imply in any way that Coachillin Holdings LLC has a direct interest or affiliation with any of the owners, tenants, and operators of cannabis businesses within the Coachillin Compound.*

1) SECURITY & CONTROL PLAN EXECUTIVE SUMMARY

The COACHILLIN' Security and Control Plan ("Plan") details all-encompassing security provisions that cover COACHILLIN' MMJ BUSINESS & INDUSTRIAL PARK tenants and their products - from cultivation, production, packaging, labeling, tracking and transportation to distribution to the licensed dispensaries. Plan provisions will comply with or exceed local laws and ordinances, the California Medical Marijuana Regulation and Safety Act ("MMRSA"), best practices from other regulated states and guidelines set by the federal government in the 2012 Cole Memorandum. All COACHILLIN' Industrial Cultivation & Ancillary Canna-Business Park ("COACHILLIN'") facilities will be operated with the safety and security of the local population, staff, and medicine as the primary concern. Understanding that there may be internal and external security threats to this property, COACHILLIN' will implement a first-of-its-kind security program to combat all known and potentially unknown threats. COACHILLIN' has anticipated threats from every arena, including but not limited to physical, cyber, and procedural security for all facilities and operations. The COACHILLIN' program is designed to give every tenant and employee the responsibility of ensuring and working within a secure environment. Our security specialists and management team have developed detailed policies and procedures, along with training programs that enhance prevention, awareness, reporting, and responsible incident management for the entire company.

EXPERIENCED SECURITY TEAM & LEADERSHIP

Working with our highly-experienced security advisors; Veterans High Risk Security Solutions, aka ("VHRSS"), a private security firm that specializes in deploying a Program of state-of-the-art security protocols. The Program will anticipate and address potential security threats, adhere to local, state and federal security regulations, including Crime Prevention Through Environmental Design (CPTED), and most importantly protect the COACHILLIN' tenants and employees. In addition to developing and implementing top-notch security practices, VHRSS will leverage their many years of Military experience in austere high-threat environments, including many years doing Diplomatic Security at U.S. Embassies around the world. COACHILLIN' along with VHRSS, will build relationships with local, state and federal law enforcement agencies to offer complete transparency into our operations and ensure compliance with all local, state and federal laws.

ADHERENCE TO HIGHEST LEVELS OF SAFETY

cultivation facilities and associated transportation and distribution program, adhere to or exceed the highest levels of safety and security within the industry. COACHILLIN' will blend various security technologies (including cameras, access control systems, bar coding, Radio Communication Systems, physical devices (security fencing, access point Delta Barriers, Motion Sensor Lighting, PA announcement system, safes/vaults, etc.), personnel, operating procedures and training to ensure COACHILLIN' properties will stand at the security forefront for all others to follow.

COACHILLIN' thru its landowners, tenants, and ex-military Security consultatns has a sophisticated understanding of medical cannabis production and general security principles. This has led us to opt for surveillance cameras covering every portion of our facilities, including all vaults and materials cited for disposal. COACHILLIN' will use sophisticated access controls that include authorized personnel-specific readers in the most restricted areas. Surveillance camera footage will be monitored at all times for anomalies within the area profile. All recorded footage will be stored in compliance with local and state regulations.

INNOVATIVE SECURITY TECHNOLOGY

Facility Cameras:

COACHILLIN' will deploy cameras that are vandal-resistant and high definition, with 5 MP progressive scan CMOS sensors, capturing 13 images per second at full resolution. Cameras will feature integrated infrared (IR) LEDs to provide uniform illumination in the dark, even at 0 Lux, up to a maximum distance of 200 feet. Cameras also feature automatic day/night functionality with removable IR cut filter that switches to day/night modes depending on the light level.

Cultivation Cameras:

Because of the documented harmful effects of basic IR light on plant growth, a highly specialized mini-bullet camera by Sony is available that uses a 940 nanometer (nm) wavelength infrared LED, which produces a glow that is undetectable to the human eye. This device offers an effective IR distance between 16 to 26 feet and is also waterproof. This camera will help reduce the effects of infrared on tenant crops. The latest technology will be provided by a sub-vendor that specializes in the cannabis industry in surveillance equipment. COACHILLIN' will compare the latest equipment and provide the best product for the site.

Fencing:

To secure the perimeter, COACHILLIN' will employ aluminum cantilever gates, access bollards and high-security anti-climb fences composed of welded wire to make cutting virtually impossible. Alternate would be 8'-10' block wall.

Intercom:

A video-intercom system will provide video security and assist in communication throughout the facilities, even from a separate location. Fully integrating systems will allow for the identification of visitors, unlocking doors, broadcasting of emergencies and announcements and forwarding of calls.

Building Access Control:

Security begins with having a professional card printer that allows for the creation of water-marked identification cards, with the option of including magnetic strip or smart card technologies. The holographic anti-counterfeiting watermark can be custom designed or use a standard design included with the system.

Contactless Smart Card Readers:

These units will be used to control access to sensitive locations. These devices combine reliability with affordability and feature enhanced 64- bit security, encryption options, superior weather resistance and anti-vandalism protection. As this plan indicates, security technology used by COACHILLIN' will consist of state of the art, commercial grade equipment. Furthermore, the security plan, along with all standard operating procedures developed, will be constantly updated and audited to guarantee that COACHILLIN' facilities remain at the highest level of security at all times.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

COACHILLIN' will use Mobile Two Man teams to monitor and patrol the outer security perimeter defined as the borders of the property. The perimeter would also be defended by natural barriers (landscaping), clearly marked with Private Property No Trespassing signage, and surveillance technology. The intermediate security perimeter will include all cultivation buildings, storage facilities and offices. This perimeter would feature man-made "stand-off zones" for primary buildings as well as physical barriers to restrict pedestrian and vehicular traffic. This intermediate perimeter would be secured by CCTV and security guards. The interior cultivation and processing facilities will constitute the inner perimeter – the proprietary zone. Walls, doors and windows become a critical layer of security. Access control to this vital zone is mandatory, requiring a visible employee identification program. All aspects of security technology have application to the inner perimeter.

COACHILLIN' will use Crime Prevention through Environmental Design (CPTED) principles to ensure that the look and feel of the production facility will enhance the surrounding environment, rather than detract from it, while ensuring there are no potential blind spots for intruders to conceal themselves. COACHILLIN' will create security measures that respect our neighbors and community and do not violate what we ourselves would not want to see or hear in our backyards.

The COACHILLIN' Security Plan lends itself to creating an environment that prohibits any theft or diversion of medical cannabis and the proceeds from their sales. Access to our facilities will be limited only to individuals with prior authorization to enter, and only on an as needed and scheduled basis.

TRANSPORTATION

COACHILLIN’ owners, tenants, and operators consider the transport of medical cannabis to be one of the most critical security risks faced. Subject to, and until there are rules and regulation to be written pursuant to local and California MMRSA, COACHILLIN’ must ensure that there are adequate layers of security on all vehicles transporting products in and out of the Compound. All products being transported will be RFID tagged and accompanied by a travel manifest that accounts for all product and the destination of that product. All routes and times of transportation will be monitored and randomized and there will be established limits capping the quantity / value of any given shipment. All security and transport vehicles will be in contact with the command and control center. In providing these multiple layers of security, COACHILLIN’ believes that diversion of its products will be virtually impossible.

2) TEAM SECURITY PHILOSOPHY

COACHILLIN’ believes the best way to approach this project is through a team approach. This team approach will be reflected throughout our security plan, but is clearly evident in the Company’s security philosophy.

COACHILLIN’ adhered to the following criteria and approach in initiating a cutting-edge security plan and in defining security goals, objectives, and techniques:

Security professionals have been involved in the project team from the earliest stages. Including the security principles in the design and development phase has allowed COACHILLIN’ to incorporate our expertise and take advantage of opportunities to use the surrounding natural and man-made environment in the physical security plan (i.e. the use of natural physical barriers and landscaping to provide access control and security shielding). COACHILLIN’’s security philosophy incorporates natural and creative landscaping to discourage or mitigate a vehicle attack on the facility without being recognized by the public as a security measure.

Environmental security strategies will include physical security design, employee/citizen and law enforcement participation in a team approach to facility security. These strategies are based on internationally known and recognized Crime Prevention through Environmental Design (CPTED) principles. These principles, which include the use of lighting, plantings, ground textures and common areas, deter crime and reduce vulnerabilities to violence and theft. The cultivation facility will strive to be a “good neighbor”, ensuring that security lighting does not become lighting pollution or serve as a source of citizen discontent. Our design includes the use of low light cameras, motion detection devices and lighting that fits into the local community.

The security design includes state-of-the-art technology, digital systems, and “all-smart” devices. All system software will utilize open architecture and protocols so that the facility is never “locked into” or dependent on a single manufacturer or vendor.

Security systems are designed to be flexible, allowing the system to cost- effectively expand and contract to meet changing needs and risk levels. Security systems management and controls will be standardized to minimize staff training requirements and reduce annual operating costs. System and equipment selection will be based on analysis of life-cycle costs rather than only initial capital outlay.

The cultivation/processing security command center will include the latest in security technology, with components that will enable the center to serve as a command post during any emergency operation.

The entire security program has been designed to prevent loss through diversion and effective risk management so that security contributes to the overall sense of cooperation within the community we serve, while ensuring our operation remains intact and secure throughout any situation.

The COACHILLIN' approach ensures these facilities will become the model for safety and security while still maintaining the sense of community required. The background and expertise of the COACHILLIN' team has provided an unmatched approach and commitment to the safety and security of our facilities.

METHODOLOGY

The scope of the COACHILLIN' Security Force Team is broad and multi-faceted. COACHILLIN' has identified and quantified the risks to a project of this type during both the construction and occupancy phases. COACHILLIN' has also taken into account the current best practices and systems within the security industry and determined which of these would be best suited to protect and secure the entire operation well into the future. COACHILLIN' focuses on all aspects of risk, including monetary, reputation, regulatory and operational risks for all constituents.

The overall methodology of COACHILLIN' segments the project into phases. Phase One encompasses the pre-construction planning stage (Assessment, Design and Preliminary Planning); Phase Two focuses on the construction stage (Vendor Selection, Exact Planning, Implementation and Documentation); and Phase Three establishes the standard operational procedures for the life of the facilities. COACHILLIN' will utilize ongoing testing, repeated threat assessment and continued development, revision and adaptation of security handbooks and protocols to reflect our ongoing commitment to facility security and the protection of occupants from evolving security and safety issues during day-to-day operations. The key to successful security in each phase, outlined below, is clear and constant communication and synergy between the COACHILLIN' Security Team, the architects, construction companies and the appropriate local, state and federal agencies.

PHASE ONE

Concurrent with developing a plan outlining functional and operational needs, the COACHILLIN' Security Force Team has been extensively involved with the project manager and architect, and this will continue throughout the life of the project and ensure that the ultimate goals of COACHILLIN' are met on schedule. In developing the blueprint during Phase One, COACHILLIN' feels that a key ingredient to the success of this project is to ensure that all construction contractors and other service providers are on the same page as our Security Force Team to ensure the development of appropriate security measures. This reduces issues that generally come up later in a project of this dimension, as the majority of those concerns will have been dealt with during the initial stages of construction. The security measures that will be considered will include all areas of each cultivation facility.

We have worked on identifying all aspects of the project that present a security risk. The Vulnerability and Security Assessment is a logical process that evaluates every aspect of the planned site, including, but not limited to, interior, exterior, ingress, egress, transportation routes, and the surrounding neighborhoods. Critical infrastructure that is an integral part of the day-to- day operation of this project will be evaluated by working closely with the appropriate authorities. Local, state and federal agencies will be included throughout the process as the need arises.

The COACHILLIN' Vulnerability and Security Assessment begins in the planning stage with a meticulous review of all available documentation, including site plans. All Security Force Team documents bring to light every aspect of security and safety including crime, diversion, terrorism, fire and medical emergencies. Continuous review and evaluation of all documents by the Security Team throughout the project development stages will include focus on systems such as fire safety, intrusion detection, etc. During this period the Security Team will build a relationship with critical infrastructure suppliers including, but not limited to, voice and data communication, power, and water.

Throughout Phase One the team will identify vulnerabilities to the facilities and the surrounding area. Every aspect of the facilities' effect on the neighborhood, from the construction phase to completion, will be taken into account. This includes public access, deliveries and utility services. Every phase of this project creates a different risk potential which must be rated for inclusion as an actionable item. The security assessment will be the springboard to developing both a state-of-the-art security program and a detailed security protocol for all situations. The assessment and testing in Phase One will continue through to the beginning of Phase Two.

PHASE TWO

As programming and schematic design begins, the COACHILLIN' Security Team, working with the project managers, will create the physical security program conceptualized during Phase One. All security design phases will be coordinated with the architect and will be incorporated in the design schedule. The role of security technology is important in today's environment, but equally critical are the operating procedures and policies surrounding those systems. These procedures embrace all day-to-day, emergency and crisis management scenarios. The COACHILLIN' Security Force Team will refine those procedures during engagement in Phase Two, using the information gained in the first phase.

COACHILLIN' will produce and continually refine detailed Security Protocol and Program Handbooks that cover the security of all structures (cultivation, command and control, storage, etc.) as well as transportation and other aspects of the operation. Long-term site security begins well before the first shovel hits the ground. A continuous review of project plans and their progress ensures that all required security measures are incorporated into the physical structure. All selected systems will undergo rigorous testing as they are installed and integration testing will occur as other systems come on- line. This ensures that all systems work together and achieve the designed goals. The COACHILLIN' Security Force Team contains specialists in deploying integrated systems and procedures for testing. Fully integrated systems and procedures testing is completed and proven before any facility opens for its intended use.

PHASE THREE

Throughout the life of the facility, the requirement to review and refine security systems and procedures is imperative. On an ongoing and random basis, the COACHILLIN' Security Team will conduct testing of alarm and other service providers as well as perform technology reviews and drills of facilities, procedures and communications. Our commitment to vigilance is unwavering.

3) GENERAL SECURITY POLICIES

The COACHILLIN' Security Force Team has designed and implemented security measures to deter and prevent unauthorized access into any of the facilities. The overall policies are designed for all areas containing medical cannabis, with a particular eye toward preventing theft or diversion at or between any affiliated or ancillary facilities. Any change made to a security protocol or procedure will be documented and distributed to all COACHILLIN' employees and any contractors or service providers that may be impacted. Training will be scheduled immediately if any procedural change is deemed to require retraining or education of staff and others.

Transportation between off-site facilities, is considered an "at risk" environment or activity for the criminal element. To that end, COACHILLIN' will fully develop a "**Prevention & Incident/Emergency Response Plan**" (P&IRP). The best way to secure and safeguard all COACHILLIN' facilities and personnel is through prevention strategies and drills. The security team assigned to protect all assets of COACHILLIN' will remain current on all phases of our security plan. In addition, all tenants and their employees at the facilities will receive specific training on how to respond to a variety of emergency circumstances.

COACHILLIN' STAFFING PLAN OVERVIEW

Outlined below is the preliminary security staffing plan for the COACHILLIN' facility. This plan will be modified as we develop the facility but our commitment will be to attract and retain only highly trained, top-notch U.S. Special Operation Veterans. COACHILLIN' will also conduct detailed and thorough training that will be reinforced by frequent security exercises and drills.

SECURITY PERSONNEL

All security personnel and employees hired by COACHILLIN' will go through specific training prior to assignment within this facility. All security personnel will be licensed in accordance with California law with respect to their specific designation and duties. COACHILLIN', will develop specific standard operating procedures (SOP's) for all security personnel, as it relates to the following:

- ✓ Hiring and Proficiency Standards Training
- ✓ Identification Standards
- ✓ Employee Management & Oversight
- ✓ Background Screening
- ✓ Drug Testing
- ✓ Random Drug Testing

The staffing plan for all phases of our project will be evaluated and the appropriate levels of security staffing will be developed and instituted as follows:

Cultivation and Production Security Personnel

The number of personnel provided by the security contractor will increase as the project is built out and reaches ultimate working capacity. During all hours of operation, a minimum of one security manager and an appropriate number security force officers will be working at the facilities. The security force manager will oversee all aspects of security and will be responsible for managing all security personnel on site as well as the transport vehicles. The security force officers will be assigned specific posts during their work day in an effort to maximize their effectiveness and the safety and security of the facility.

Transportation Security Personnel

COACHILLIN’ considers the transport of medical cannabis to be a critical security risk. Until the State of California licenses transporters and establishes protocols for the transportation of medical marijuana, COACHILLIN’ will ensure security protocols extend to all transport vehicles used by the producing tenants at our facilities. The transportation of all medical cannabis products will follow developed security and “track and trace” protocols. Transportation vehicles will always carry system generated travel manifests showing the product being transported and the final destination of the product. All products will be packaged and inventoried with a Radio Frequency ID (RFID) tag and will be monitored to ensure correct routing and a safe and timely delivery. All destination dispensaries will be connected to Guardian Data Systems’ ROAR compliance track & trace system database, with all product being properly inventoried at every step of the chain of custody from seed to sale.

COACHILLIN’ will develop requisite equipment and security measures so that all vehicles are equipped with communications and security to provide safe delivery for the transporting employee and product being transported. Post orders will be developed with detailed and explicit duties and responsibilities for each post and assignment. Additionally, a prevention and incident emergency response plan has been developed for a variety of potential emergency situations.

GENERAL PREVENTION MEASURES

- ✓ Continuously monitored, multiple point facility entry / exit.
- ✓ The main vehicle entry / exit will be equipped with a guard post and guard activated security gate.
- ✓ All vehicles entering and exiting the facility will be subject to inspection and search.
- ✓ Admittance by scheduled appointment only. Verified by contact from Command & Control Center to tenant management. An allotted visit time maximum will be enforced to limit the number of visitors on site at any time.
- ✓ All deliveries and shipments will be monitored by security personnel.
- ✓ Employees will be trained on proper procedures for opening and closing facilities.
- ✓ Employees will be trained on proper handling of access control devices.
- ✓ Transportation of medical cannabis will follow irregular delivery routes and times.
- ✓ Transportation may, in addition to travel manifest and RFID, be monitored by GPS, CCTV and computer.
- ✓ Employees will be trained in proper handling of cash if needed.
- ✓ CCTV systems will be designed to capture all individuals entering and exiting COACHILLIN’ facilities from multiple angles to prevent shielding of identity with hats, hoods or other articles of clothing.
- ✓ All facilities will be well maintained both inside and out.
- ✓ All facilities will be effectively lit, both internally and externally.
- ✓ Utilization of the CPTED principles for our environmental design.
- ✓ Employees will be trained on anti-diversion techniques.
- ✓ Employees will be trained on how to identify suspicious persons or activity.

- ✓ Employees will be trained on how to respond to a variety of emergency situations from active shooter to general medical emergencies.

INCIDENT RESPONSE MEASURES

- ✓ Employee training on the P&IRP is critical to properly respond to key incidents, including but not limited to:
  - Robbery
  - Burglary
  - Intruders in Coachillin' Project
  - Threats of violence in Coachillin' Project
  - Assaults
  - Weapons possession
  - Civil
  - Flood – natural or manmade
  - Proper use of panic, burglar alarms
  - Cyber security
  - Proper response when law enforcement or first responders arrive at facility
  - Incident reporting

COMMUNICATION WITH LAW ENFORCEMENT

COACHILLIN', in conjunction with the security manager, must maintain a list of non-emergency police department contacts for all facilities. The security manager must maintain regular communication with each law enforcement contact, advising of any changes in security policies or procedures. COACHILLIN', through its Security Team, will maintain strong partnerships with local, state and federal law enforcement agencies. The security manager shall engage these agencies to support the security mission through:

1. Proactive meetings
2. Observation patrols
3. Rapid response to incidents
4. Collaborative training and exercises

SECURITY AUDIT SCHEDULE

COACHILLIN' will perform audits to ensure compliance in accordance with the Compliance and Audit Plan. In addition, the COACHILLIN' Security Team will conduct testing randomly throughout all facilities. This testing will include attempts to enter facilities outside of the above-outlined procedures. COACHILLIN' security assets will remain constantly alert for any sign of employees who are willing to violate these procedures or for any flaws in COACHILLIN' security protocols that might allow unauthorized visitors into one of our facilities.

WASTE PRODUCTS/BYPRODUCTS DISPOSAL

Medical Marijuana/Cannabis Waste Byproducts

COACHILLIN’ understands that throughout the process of growing marijuana there is a certain amount of waste product that will be created. COACHILLIN’ will comply with all local and state laws promulgated by the MMRSA with regard to disposal of waste products. Until such rules and regulations are codified, all waste products will be logged in the management system. Even though it is believed that the majority of the waste product (plant root ball, extracted marijuana plant material and stems, etc.) produced has no THC or other cannabinoids of significance remaining, COACHILLIN’ will treat all such byproducts with extreme care and diligence.

1. All waste plant material will be visually inspected and then rendered harmless by designated personnel before it is loaded into waste disposal containers. The employee will make a log entry regarding that inspection.
2. All waste containers will be maintained within the secure facility, and will be equipped with locks and tamper resistant seals until they are removed by an authorized waste disposal company.

SECURITY OPERATION CENTER (SURVEILLANCE)

The COACHILLIN’ Security Operations Center (SOC) will allow the Security Team to monitor all activities in and around the facilities in real-time. Security Operations Center rooms will remain locked at all times and will not be used for any other function. Access to the SOC will be controlled by the Security Manager and will be limited to authorized personnel only, as indicated below:

1. Security persons who are essential to surveillance operations
2. Law enforcement authorities acting within their lawful jurisdiction
3. Security system service personnel – A current list of all authorized providers will be maintained, and updated on a regular basis
4. The current list of authorized employees and service personnel who have access to the Security Operations Center must be maintained by the security manager and will be available to appropriate authorities upon request.

COMMAND & CONTROL CENTER

COACHILLIN’ has designed our Security Operations Center to continuously monitor any activities relating to the cultivation and transport of certified medical marijuana. Our Security Operations Center will be staffed 24/7.

A sufficient number of security force officers based on the phasing of the project, will staff this location at all times, and will continuously monitor the security entrance gate and all Coachillin’ and transport vehicles.

4) COMPLIANCE & ACCOUNTABILITY

"SEED TO SALE" MONITORING WITH ROAR (POWERED BY GUARDIAN DATA SYSTEMS)

Executive Summary

COACHILLIN' will utilize a ROAR, a full featured third party ERP solution developed by Guardian Data Systems for all track & trace regulatory requirements at both the municipal and state levels. This solution will give the City of Desert Hot Springs ("City") and COACHILLIN' the ability to monitor and track activity without full-time dedicated compliance staff, while maintaining compliance above and beyond industry standards. The monitoring ability of the ROAR platform will be able to send predetermined non-compliance or warnings for incidents that happen outside of the regulatory parameters. COACHILLIN' has enlisted the services of Guardian Data Systems and their ROAR platform to ensure a framework of compliance that will function on its own, and also allow for monitoring by regulatory compliance heads of the state and the City of Desert Hot Springs. The State of California compliance framework has yet to be established, and the ROAR platform will ensure that we will operate to meet the current guidance given by the United States Department of Justice when California implements regulatory frameworks for both medical and soon recreational sales of marijuana. Deployment of the ROAR system will provide a "closed loop" process and system that will ensure compliant participants at all points in the chain of custody for all operations within the Coachillin Park, as well all affiliated canna-businesses located elsewhere in the state of California.

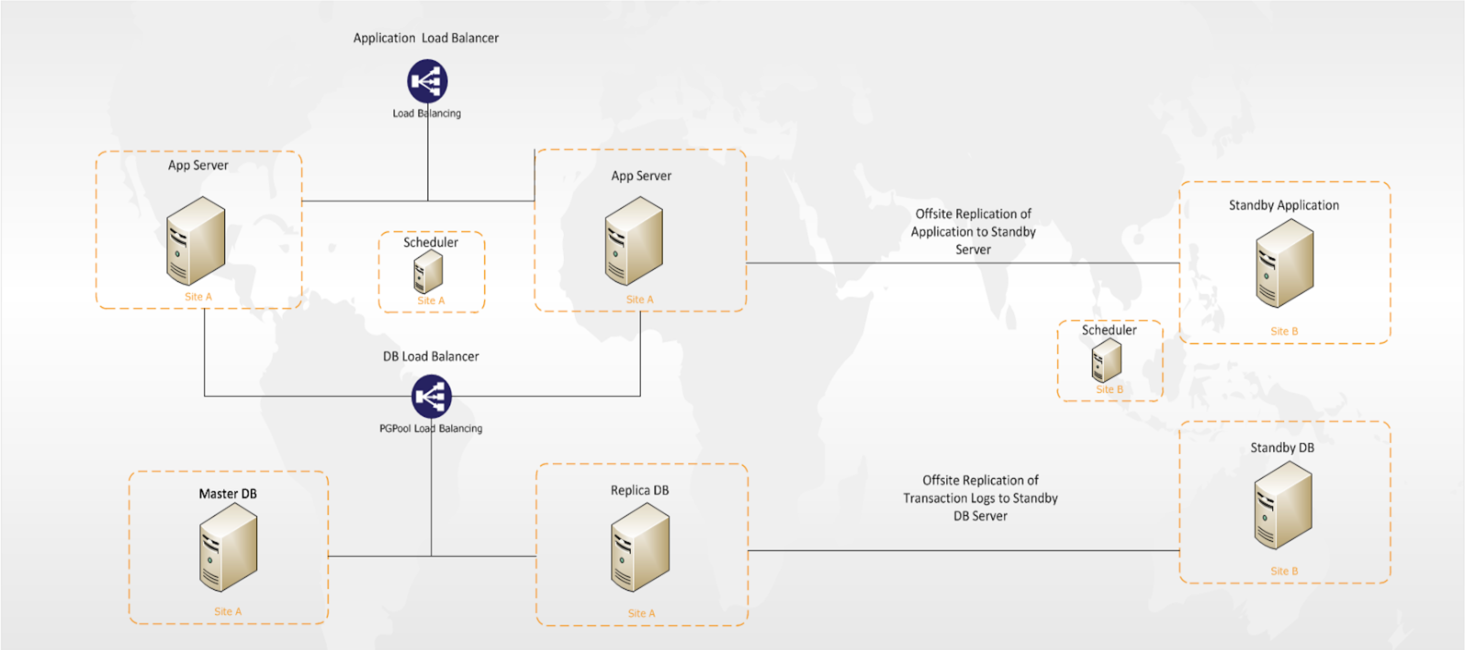
Guardian Data Systems business management system, ROAR, provides mature business management software for cannabis enterprise organizations. ROAR has been in production use with large retailers, distributors, and manufacturers for more than a decade, and the Guardian Data Technology team is deeply experienced in successfully migrating companies to efficient operations through the use of ROAR.

The ROAR Platform: At-A-Glance

- All operators running cannabis cultivation/processing/manufacturing/production facilities will submit to a background check and will be registered in the system.
- All destination dispensaries will be registered operators and have background checks done to include validation of their ability to operate within their jurisdiction.
- All cultivation will be RFID tagged at the individual plant level and all plants will be monitored and controlled from the early stages of growth to harvest.
- All production will be RFID tagged and all packages will be logged out and into inventory.
- All transportation of product will be manifested and monitored from the origin to the destination.
- Instant notification, by email or text, of all significant events.
- Robust secure system data storage, providing reports of all Medical Marijuana products produced and where deliveries and sales are made.
- All information about production within the closed loop available to City management and local law enforcement.
- Ability exists for additional fees/revenues that can be collected through plant and product tags.

Data Security & Technology

ROAR's scalable transactional database architecture provides performance driven, on-demand (24 x7) and real-time access from anywhere, while allowing configurable workflows, approval processes, business rules, reporting tools and user windows. Below is a visual representation of our Amazon Web Services hosted application hosting architecture.



Infrastructure Reliability

- ✓ Business application processes provide 24 x 7 availability and security.
- ✓ Data is securely replicated on redundant servers and databases.
- ✓ Uninterrupted Power Supply (UPS) provides power during outages.
- ✓ Fire detection and suppression systems are employed in the data centers.
- ✓ Climate control systems maintain a constant hardware operating environment.
- ✓ Constant monitoring quickly identifies and responds to systems problems.
- ✓ Preventative maintenance maximizes performance and life of hardware systems.
- ✓ Proactive measures protect data from attacks.

Data Center Details

- ✓ Access to data centers is monitored and kept secure with surveillance systems, intrusion detection systems and professional security 24/7.
- ✓ Applications are protected from unnecessary access, allowing only appropriate services through the firewall.
- ✓ Data transmissions are encrypted with 256-bit Secure Socket Layer (SSL) Certification and follow the standards required by the PCI-DSS (Payment Card Industry Data Security Standard).
- ✓ Stringent password policies prevent unauthorized access to applications.

Guided Implementation

For all of Guardian Data Systems customers, we provide a full ROAR guided implementation process. To begin the implementation process, a Guardian Data Systems (GDS) project manager works directly with the customer to export data and import all pre-existing data into ROAR. This data is reconciled with the inventory and financial data the city/county/state has on file for that customer and any discrepancies are resolved immediately prior to going live with ROAR.

After the historical data is imported, GDS activates the respective batch/lot, barcode or RFID inventory management methodologies the customer is utilizing at their location. All scanners are tested for accuracy and the respective data is received through the ROAR interface. Inventory is allocated to respective warehouses or rooms in the system and ROAR can track product down to the aisle, row, shelf, bin, and individual inventory record. Data is also stored in ROAR regarding the purchase history of the inventory. At any time the customer can view an inventory record, see if that inventory is a simple material, bulk, or finished good bill of material (BOM). The customer is also able to see which vendor the product was purchased from. This data is recorded for all vendors within the product life cycle tracing the inventory back to the cultivator and the original plant the cultivator produced. In the case of a product return and recall, the customer can scan the product and find the product record or search for the product by product name and when it was sold or whom it was sold to. The customer can then identify all vendors who interacted with that product and all other inventory that is from the same batch as the product that is being recalled.

In addition to inventory data sets, ROAR provides data fields and attributes for tracking temperature, humidity, ventilation, water supply, lighting, equipment maintenance and other custom attributes the customer would like to track. These attributes can then be reported against to identify important production metrics that may affect the plant, batch or finished good. All inventory, purchasing, sales, vendor, customer/patient, inventory movement, production attributes and compliance data is stored in real time through the customers ROAR instance and related database. If the customer has multiple locations, the data can be segmented on a per location basis and aggregated into a parent instance for ultimate organizational oversight. ROAR provides time stamped transaction logs and historical data that is never deleted for internal auditability. Data is also backed up to redundant server locations in separate cloud data warehouses in segmented geographical regions to ensure system uptime, security and data recovery. In addition to data transacted through ROAR and stored in the ROAR cloud environment, the customer has the ability to download the data locally.

COMPLIANCE & TRACEABILITY

ROAR has an open API that connects to internal system data points. When inventory (Plants, Clones, Nutrients, Bulk Inventory, Simple Inventory, Finished Goods etc.) is produced, moved, wasted, purchased or sold, ROAR utilizes those data points and automatically formats them into city/county/state specific reporting formats. Via API, ROAR can send all traceability event data directly to the city/county/state/country selected regulatory system. This can occur in real time or batched on a particular cycle (example: Daily). In addition to API communication with municipal compliance systems, ROAR is capable of providing data exports that the customer can upload to any municipal compliance system. To ensure customer confidence and compliance, Guardian Data Systems also provides proprietary physical inventory tools that can identify internal inventory discrepancies or differences between physical inventory and the data held within the city/county/state regulatory system.

5) EQUIPMENT MAINTENANCE

The Security Manager or authorized agent will schedule and oversee the required maintenance of all security equipment in accordance with manufacturer recommendations. Should any equipment be found defective, it will be corrected immediately.

ANNUAL SECURITY SYSTEM AUDIT REQUIRED

A security system audit by an approved independent vendor will be conducted on an annual basis. Should the audit identify issues related to the COACHILLIN’ security system, steps will be taken to address those concerns within 10 business days of the findings.

REPORTING REQUIRED

All COACHILLIN’ employees are required to immediately report any of the following incidents to the Security Manager:

1. Any alarm activation or other event that requires response by law enforcement or security personnel
2. The failure of any security alarm system due to a loss of power or mechanical failure that is expected to last longer than four hours
3. Inconsistencies identified during inventory or any diversion, theft, loss or criminal activity suspected at the cultivation facility
4. Unapproved destruction of medical marijuana, whether accidental or otherwise
5. Any loss or improper alteration of records related to medical marijuana cultivation or transportation, including personnel records
6. Any other breach of security, suspected or actual.

6) COACHILLIN’ ACCESS CONTROL PLAN

All means of access control (keys, alarm codes, access control cards, etc.) in any COACHILLIN’ facility will be strictly controlled and monitored to ensure that no unauthorized persons can access the facility. COACHILLIN’ has established multiple layers of security to prevent any and all breaches, including closed circuit television, access control readers, alarm systems, vaults, etc. Employees will be issued access control credentials, limiting their admission to only the areas of the facility their job description requires.

FACILITY ACCESS - EMPLOYEES / VISITORS / VENDORS AND LIMITED ACCESS AREAS

COACHILLIN’ has developed a comprehensive policy regarding all Identification Badges and Visitor Policies, which aim to prevent unauthorized access to any COACHILLIN’ facility. The security measures outlined in this document will ensure an environment that effectively precludes unauthorized access to any COACHILLIN’ medical marijuana facility. The policy clearly defines the employees, contractors and visitors who will have authorized access to individual facilities as well as designated limited access areas.

The security measures outlined in this document have been put in place to protect all employees and facilities from potential harm, both physically and financially. COACHILLIN' has identified specific personnel who are authorized to distribute permanent and temporary identification badges, along with the stringent process they must adhere to in doing so. Identification badges are assigned based on category of employees, vendors, contractors, and visitors. Identification badges are further restricted based on necessary areas of access, with different levels of access clearly defined for ease of identification by employees and security personnel. The policy clearly defines provisions for displaying identification badges and the handling of lost or stolen badges.

Only authorized visitors will be allowed access to the Coachillin' Park. All vendors, contractors, and visitors must obtain permission to enter a COACHILLIN' facility 24 hours prior to arrival and, upon arrival, will be issued an identification badge. Visitors will be escorted at all times by a designated tenant or COACHILLIN' employee.

EMPLOYEE, VENDOR, CONTRACTOR AND VISITOR IDENTIFICATION BADGES

Categories of badges for entry into a COACHILLIN' facility

1. Tenant and COACHILLIN' employee badges.
2. Temporary badges for vendors and contractors.
3. Visitors badges.

IDENTIFICATION BADGE POLICY (GENERAL)

The purpose of COACHILLIN' Identification Badge policies and procedures is to enhance the security and safety of employees, vendors, contractors and facilities from potential harm, both physically and financially. Each employee, contractor and visitor is responsible for the safekeeping of his or her badge once it has been issued. COACHILLIN' security personnel will instruct and ensure compliance by all persons entering any COACHILLIN' facility on the proper handling, safeguarding and retention of their identification badges. Tenants, vendors, contractors and visitors will be instructed by security personnel that their ability to maintain a relationship with the COACHILLIN' facility is subject to forfeiture should they violate the identification badge policy and requirements.

IDENTIFICATION REQUIRED FOR ENTRY INTO ALL COACHILLIN' FACILITIES

For each vendor, visitor, and contractor that requires access to the facility, COACHILLIN' will collect and hold a form of identification (driver's license, official badge, etc.) in exchange for a temporary issued visitors badge. The issued badge must be clearly displayed by the visitor at all times while on facility grounds. All visitors will be required to be escorted by the authorized sponsor and not be left unattended at any time. All visitor badges will be returned to the COACHILLIN' ECP before exiting the facility. A visitor request form, to be filled out by a Coachillin' sponsor, must be submitted to the SOC seven (7) days prior to the visit. Visit approval will be granted through established security protocol.

During all hours when the business is not operating the Security Manager will ensure that all entrances to and exits from a licensed premise are securely locked and any keys or key codes to the enclosed area remain in the possession of the licensee, licensee representative, or authorized personnel.

Access to secure areas will be given only to individuals where need can be demonstrated. The General Manager and Security Manager have ultimate responsibility for issuing access. Issuance must be recorded by the issuing individual, including documentation of any facility keys, alarm codes, electronic access codes, passwords, or combination codes.

Keys and electronic access codes must be protected. They may not be loaned and should not be left unattended. All keys and access cards issued to employees should be retained in the possession of the employee to whom issued and may not be transferred directly from one employee to another.

Employees must report any lost keys or access cards to his or her manager immediately. The general manager along with the security manager will make a determination as to whether the system has been compromised and whether re-keying will be necessary. It is against company policy to duplicate keys, share passwords, or share access codes.

Should the Company choose to utilize electrified access hardware, it will have a failsafe (keys) in case of a power outage, and the system will remain in a fail secure position in the event of a power outage.

ISSUING AUTHORITY

Employee, Vendor and Contractor Badges:

The COACHILLIN' Security Manager will issue all appropriate badges with access restrictions based on need.

Visitor Badges – Pre-approval & Emergency Access:

COACHILLIN' policy prohibits the entry of any visitor who has not received a pre-approval, except in the event of emergency.

An emergency circumstance would include a maintenance issue, such as broken plumbing or HVAC that would require immediate contractor action on site. In either case the Security Force Manager, or their designee, will issue a visitor badge. A designated Security escort will provide over watch for the duration of the emergency situation.

Visitors to the premises shall be logged in. No one under the age of 18 will be allowed on the premises. The visitor log shall include Visitor name, DOB, government issued identification (ie: driver's license), date of visit, duration of visit, purpose of visit, and name of person visiting.

COACHILLIN' IDENTIFICATION BADGE AND ACCESS PROCEDURES

All employees accessing Coachillin' will be held to the highest standard as it relates to the security and safekeeping of their identification badges.

All tenant employees will adhere to the following:

1. Upon arrival at the ECP at the COACHILLIN' facility, each employee will exchange a government issued ID

for their COACHILLIN’ facility badge.

2. Only authorized employees of the specific tenant facility will be allowed access to the site. No other tenant employees (from another location, etc.) may enter a COACHILLIN’ facility without prior written authorization from the Security Force Manager.
3. All employees must wear their issued identification card while on the COACHILLIN’ facility.
4. The identification badge must be visible to others at all times while on the COACHILLIN’ facility.
5. When entering any access-controlled area, employees must not allow entry of another person (employee or otherwise) unless the individual displays a proper identification badge and has clearance to the controlled area.
6. Only COACHILLIN’ authorized badge display devices (lanyards, lapel/pocket clips and armbands) are permitted.
7. Under special work conditions, the Security Force Manager may modify display practices. Although it is impossible to identify all the special work conditions that might require a modification to our badge display policy we have included one here. A flood condition (broken water main) that requires long hours working in a wet environment where the badge may be damaged due to over exposure.
8. Employees must never depart the COACHILLIN’ facility with their COACHILLIN’ badges to maintain an accurate account of employees that are on the facility for accountability in an emergency situation.
9. Employees must never loan their identification or access control devices to anyone, even an authorized employee.
10. Employees must never leave their access control devices unattended, unless secured.
11. Any employee who resigns or is terminated will immediately return his or her identification badge and any other access control devices.
12. All identification badges belonging to any employee who resigns or is terminated will be immediately deactivated and properly disposed of by COACHILLIN’ security personnel at time of separation from service.
13. Non-compliance with these policies or any breach of COACHILLIN’ security procedures must be reported immediately to the Security Force Manager or their designee.
14. Violation of this policy will lead to stringent disciplinary action, including termination.

TEMPORARY BADGE PROCEDURE FOR COACHILLIN’ EMPLOYEES

When an employee has forgotten his/her identification. Their immediate supervisor will be contacted and required to respond to the ECP or their designated representative to sign the employee in who then will be issued a temporary identification badge.

LOST OR STOLEN BADGE PROCEDURE FOR COACHILLIN’ EMPLOYEES

Any employee who loses his or her identification badge or has it stolen must immediately contact their employer and the onsite Security Force Manager. The lost identification card will be immediately deactivated and removed from the system by the COACHILLIN’ Security Force Manager. The Security Force Manager will ensure an incident report is filed regarding each lost or stolen badge. A weekly report of any lost or stolen badge will be generated for review by the Security Director.

COACHILLIN’ VISITORS IDENTIFICATION BADGE PROCEDURES

A visitor is any individual who is conducting business in a COACHILLIN’ facility other than an authorized employee. All visitors must be issued a visitor identification badge upon entry into any COACHILLIN’ facility. These badges will be for identification purposes only and will not be programmed for access to any areas within Coachillin’. For purposes of this procedure, COACHILLIN’ will adhere to separate protocols for two categories of visitors: (1) Authorized Visitors, (2) Vendors and Contractors.

Authorized Visitors

Tenants, with COACHILLIN’ approval, may authorize a visitor to their cultivation operation. COACHILLIN’ security personnel will record each visit in the visitor log and adhere to all procedures described below regarding authorized general visitors. All visits will be scheduled in advance and COACHILLIN’ will stagger appointments to control the number of visitors on site at any given time.

Vendors and Contractors

A vendor or contractor is a supplier, professional service representative or consultant (contractor) who has business with COACHILLIN’. All vendors and contractors, who service facilities in the Coachillin’ Park, either long term or on a one time basis, must be properly vetted by COACHILLIN’ security and approved for entry in our facilities. Except in cases of emergency (e.g., broken utility, water pipe, electrical, HVAC system failure, etc.), neither a vendor nor contractor will be permitted access to any COACHILLIN’ facility without prior approval. The Security Force Manager will allow a vendor or contractor access to a COACHILLIN’ facility only after ensuring that prior tenant approval has been given or after documenting the emergency circumstances.

Visitor Sign In Procedure

1. Pre-approval is required for all visitors, except in emergency. Emergency circumstances are true emergencies and this exception shall not be used as a “catch-all” to allow unauthorized individuals into any COACHILLIN’ site. Examples of real emergencies include, but are not limited to, a mechanical failure that could affect the cultivation facility such as an HVAC breakdown, flooding due to plumbing failure, fire, etc.
2. The COACHILLIN’ ECP will approve entry by a visitor only after ensuring that proper approval was granted or after documenting the specific emergency circumstances.
3. Government identification (e.g., driver’s license, agency ID card, etc.) is required for any visitor entry into a COACHILLIN’ facility.
4. All visitors will be issued a visitor identification badge, along with the appropriate holder that is to be worn around their neck. Visitors must display their visitor identification badge at all times while in the facility.
5. All visitor badges will be for identity purposes only and will not be programmed for access to any area in any COACHILLIN’ facility.
6. All visitors will be escorted by the appropriate tenant, designated agent or security agent and will never be left unattended at any time. Any visitor who requires appropriate access to a restricted access area must have specific permission to visit a particular area of the facility and be escorted at all times.
7. All visitor badges must be returned to COACHILLIN’ security ECP before exiting the facility.

8. No temporary badges will be issued for more than one day.
9. Any employee who observes anyone on a COACHILLIN' facility without a proper identification badge has a duty to question the individual as to their purpose for being in the facility and to see the appropriate identification badge. Should anyone be found in a COACHILLIN' facility without the proper identification badge, employees are responsible for immediately notifying COACHILLIN' security force personnel.

Lost Visitor Badge

When a visitor reports losing his or her visitor badge, COACHILLIN' security will record the information in the visitor log. For each lost visitor badge, the Security Force Manager must file an incident report. A weekly report of any lost or stolen badge will be generated for review by the Security Director.

Visitor Log

COACHILLIN' will maintain an electronic visitor log for each visitor who enters any COACHILLIN' facility.

Storage of Identification Badges – Pre-Issuance.

Any and all forms of identification badges to be issued by COACHILLIN' must be secured in a locked safe until such time as they are issued. The safe will be located in the Security Operations Center. All unused badges will be accounted for on a daily basis. A record of this daily inspection will be kept in the daily security log.

7) VIDEO MANAGEMENT SYSTEM

A Video Management System (VMS) will be deployed throughout the COACHILLIN' facility. The actual configuration of VMS will be solely dependent on the planned layouts for the cultivation facilities. However, all VMS control equipment will be located at the Security Tactical Operations Center and include a server, recording servers, workstation, and system software, as required to meet the video system requirements. This provides for around the clock redundant recording.

At a minimum, the head end equipment will meet the following performance specifications:

1. All cameras at all locations will be recording 24 hours per day, 365 days per year.
2. All recorded camera images will be retained for a minimum of ninety (90) days. Security Tactical Operations Center will also have storage available to segregate and store any recording that is part of an investigation for an indefinite time period.
3. All cameras will be recorded at a minimum of 15 frames per second (fps) using the latest technology in video compression. Although 30 fps is a high-quality standard, frame rates as low as 15 fps can still produce acceptable quality video images. However, our VMS Recording Plan will be designed to accommodate 30 frames per second or 'real-time' recording.
4. Redundant recording servers shall be employed to ensure image retention.
5. All recording that is part of an investigation will be able to be permanently archived both on the server and on recording media.
6. All VMS Systems deployed will have the ability to immediately produce a clear color still photo that is a minimum of 9600 dpi from any camera image from live or recorded images. As part of the VMS Plan,

Photo Printers will be arranged in each location's VMS System Design to achieve this requirement.

7. All security video recordings will have an embedded date and time stamp. The date and time will be synchronized and set correctly and will not substantially obscure the picture.
8. All VMS Systems deployed will have the ability to remain operational during a power outage. Emergency power generation provisions will be made at to effect this requirement.
9. All video recordings produced by the VMS System will be capable of exporting still images in an industry standard image format (including .jpeg, .bmp, and .gif). Exported video will have the ability to be archived in a proprietary format and be digitally watermarked. A digital watermark is a digital signal or pattern inserted into a digital image's unaltered copy of the original image and ensures authentication of the video and guarantees that no alteration of the recorded image has taken place. Exported video shall also have the ability to be saved in an industry standard file format that can be played on a standard computer operating system. All video recordings will be erased from the respective VMS in the event that a facility is sold or disposed of.
10. In the instance of a pending criminal, civil or administrative investigation or legal proceeding for which a recording may contain relevant information, COACHILLIN' will retain an unaltered copy of the original recording until the investigation or proceeding is closed or the entity conducting the investigation or proceeding notifies the registered organization that it is not necessary to retain the recording.

Security Video Cameras

In accordance with the COACHILLIN' Security Video Cameras (SVC) plan, cameras will be positioned in strategic locations throughout the facility to monitor activity in all areas.

The video surveillance system will be designed with a failure notification system that provides an audible, text or visual notification of any system failure. The failure notification system will provide an alert to the facility within five minutes of the failure, either by telephone, email or text message.

All cameras will, at a minimum, be Internet Protocol (IP) High Definition resolution cameras producing forensic or evidentiary quality images. Megapixel cameras will be deployed in certain areas as necessary to produce forensic quality images. The SVC plan will use the latest camera technology in surveillance systems and components currently available. Camera technologies that will be taken into design consideration will include:

- ✓ High Definition (HD) and Megapixel Network Cameras have an important role to play in video surveillance applications. They can provide images that are more useful, with more image detail and with wider coverage than standard resolution cameras.
- ✓ Thermal Network Cameras outperform a visual camera in dark settings and are an effective element for detecting people and objects in 24/7 surveillance, from pitch dark areas to a sunlit parking lot and other challenging environmental conditions. Thermal network cameras create images based on the heat that radiates from any object, vehicle or person. A thermal camera is less sensitive to problems with light conditions, such as shadows, backlight, darkness and even camouflaged objects. These cameras deliver images that allow the Command and Control Center operators to detect and act on suspicious activity. However, as thermal cameras do not provide images that allow reliable identification, COACHILLIN' will complement probable thermal camera locations at the cultivation facility with High Definition (HD) and Megapixel Network Cameras and support each other in a surveillance installation.

VIDEO SURVEILLANCE EQUIPMENT

Coachillin' intends to install a video surveillance recording system that will be operational at all times. Surveillance system will include technology (cameras and software) that will allow for generating images capable of capturing facial detail in designated areas.

The system is equipped with a failure notification system that provides, within one hour, notification to the licensee or an authorized representative of any prolonged surveillance interruption or failure.

The system has sufficient battery backup to support itself the event of a power outage.

The system meets the following requirements:

- The video surveillance system is capable of recording all pre-determined surveillance areas in any lighting conditions.
- The video surveillance equipment and recordings are stored in a locked secure area that is accessible only to the licensee, licensee representatives, or authorized personnel, and the Commission.
- In all areas where marijuana may be present, all cameras shall have minimum resolution of 1280 x 720 px and record at 10 fps (frames per second). Cameras will also be placed strategically throughout the facility to ensure facial recognition where necessary.
- System is equipped with software allowing local authorities to login in to cameras remotely in the event of a major incident.

CAMERA COVERAGE AND CAMERA PLACEMENT

Cameras will be placed to cover all areas where a marijuana item is produced, processed, stored, weighed, packaged, labeled etc. All points of entry to or exit from limited access areas; and all points of entry to or exit from the licensed premises. Cameras will also be placed in rooms with exterior windows, exterior walls, roof hatches, or skylights and storage rooms, including those that may contain safes. Coverage will also include the security room in which the server and network infrastructure are located.

All cameras will be placed so that they capture clear and certain images of any individual and activity occurring within 20 feet both inside and outside of all points of entry to and exit from the licensed premises; and anywhere within secure or limited access areas on the licensed premises.

VIDEO RECORDING REQUIREMENTS FOR LICENSED FACILITIES

Camera Specifications

Video resolution will be at least 1280 x 720 pixels and have the date and time embedded on all surveillance recordings without significantly obscuring the picture.

The surveillance system will also have the capability to produce a still photograph from any camera image.

Coverage Specifications

The licensed facility will be equipped with cameras that provide full coverage of the facility including all interior spaces where marijuana items will be present.

At minimum, the facility will have cameras placed so that they capture clear and certain images of any individual and activity occurring: within 20 feet both inside and outside of all points of entry to and exit from the licensed premises; and anywhere within secure or limited access areas on the licensed premises.

Cameras also cover exterior spaces including at all points of entry and exit including exterior windows.

The video coverage shall be audited on a periodic basis to ensure that all cameras are in good working condition, and coverage areas are covered at all times, both before and after inventory, equipment, and furnishings are in place.

Video Archive and Retrieval

Surveillance system will be equipped to retain a minimum of 30 days of continuous recording data from every camera installed at the licensed premises. Data will be easily accessible in the event that footage is requested.

All archived required records not stored electronically in a locked storage area. Current records may be kept in a locked cupboard or desk outside the locked storage area during hours when the licensed business is open.

Archive video recordings in a format that ensures authentication of the recording as a legitimately-captured video and guarantees that no alterations of the recorded image have taken place. Videos can be easily accessed for viewing from security, law enforcement, the commission, or a facility employee upon request.

If the licensee has been notified in writing by the Department or its authorized agents, law enforcement or other federal, state or local government officials of a pending criminal or administrative investigation for which a recording may contain relevant information, the grower/processor shall retain an unaltered copy of the recording until the investigation or proceeding is closed or the entity conducting the investigation or proceeding notifies the grower/processor that it is not necessary to retain the recording.

Surveillance system will be equipped with redundancy and/or offsite backup to mitigate any risk of tampering with video footage. Video surveillance records and recordings available immediately upon request.

Maintenance and Outages

Company will engage with a security provider to provide, install, maintain, and if required, monitor the video footage.

Should there be any equipment failure or system outage, the General Manager and Security Manager shall be notified immediately, and they will be responsible for coordinating the repair or restoration of the system.

LOCATION AND MAINTENANCE OF MONITORING EQUIPMENT

All premises will have a surveillance area in an office that may be accessed only by the General Manager, the Security Manager, or their licensed assignees as needed. Assignees include state or local law enforcement agencies, Commission employees, and authorized service personnel or contractors. Security Manager will keep an updated list of employees or contractors who have access to surveillance area, and will make it available the Department upon request.

Entrance to the office shall be locked whenever the office is not in use, and accessible by a key or electronic keying system.

Recording equipment will be stored in the office, in a separate locked cabinet or in the vault. The Company shall also utilize a redundant offsite feed which will also meet any requirements issued by the Commission. All recordings, including current and archival, will be easily accessed for viewing and easily reproduced.

The General Manager will maintain a current list of all authorized employees and service personnel who have access to the surveillance system and room on the licensed premises.

The Security Manager will keep a surveillance equipment maintenance activity log on the licensed premises to record all service activity including the identity of any individual performing the service, the service date and time and the reason for service to the surveillance system. Security manager will also ensure that all equipment is inspected by an authorized security vendor at least once a year.

Security Manager will keep a detailed log and records of all maintenance, inspections, alterations and upgrades performed. Records will be kept for a minimum of 3 years.

If the licensee has been notified in writing by the Department or its authorized agents, law enforcement or other federal, state or local government officials of a pending criminal or administrative investigation for which a recording may contain relevant information, the grower/processor shall retain an unaltered copy of the recording until the investigation or proceeding is closed or the entity conducting the investigation or proceeding notifies the grower/processor that it is not necessary to retain the recording.

In the event of a mechanical malfunction of the security or surveillance system that exceeds an eight-hour period, the Security Manager shall notify the Department immediately and, with Department approval, provide alternative security measures that may include closure of the facility.

8) INTRUSION DETECTION SYSTEM (IDS)

FACILITY ALARM SYSTEMS

The licensed premises will engage the services of a third party (i.e. the VHRSS Coachillin Security Team and/or their designee) security company to install, maintain, and monitor an alarm system that is activated at all times that the business is closed. The system will detect unauthorized entrance at all entry or exit points (including roof hatches), and all exterior windows (including skylights) of the premises.

Alarm system will also detect movement in all required areas within the licensed premise when the premises is vacant of employees. This will be accomplished through the use of passive infrared motion detectors place throughout the facility.

The alarm system will be programmed to notify the central Security Operations Center (SOC) who will notify the General Manager and Security Director, or its authorized assignee, in the event of a breach. If unavailable, law enforcement will be contacted and dispatched.

Alarm system is equipped with a system failure notification that will notify via email, phone, text, or a combination of those methods that will trigger notifications in the event of any system failure, including, but not limited to, power outage, loss of supervision, or connectivity issues.

An uninterrupted power supply will be installed to allow the alarm system to remain active in the event of a power outage that meets or exceeds mandated time frames set forth by state and/or local ordinance.

Upon request licensees shall make all information related to security alarm systems, monitoring and alarm activity available to the Coachillin' Security team (VHRSS) or regulatory body.

Duress Codes & Panic Procedures

All employees will be assigned a 4 digit "duress" code. In the event of an emergency, such as an employee is being forced to "disarm" a system by an intruder, by entering the duress code, the alarm system will trigger a "silent" alarm that will notify the appropriate personnel of a breach, as well as dispatch authorities.

Panic buttons will be located throughout the facility to enable staff to trigger an alarm in the event of an emergency. Once pressed, the panic buttons will immediately send text and email alerts to all parties involved and alert the central station. Triggering a panic button will also sound an audible alarm.

Secondarily, there will also be panic buttons placed strategically throughout the facility that will trigger a "silent alarm," similar to the sequence of events when a duress code is utilized.

System keypads will be located at the front entrance area and the Security Tactical Operations Center. Doors that are emergency exit only or are not part of everyday usage will be monitored at all times.

1. Panic alarm buttons will be installed in the following areas that will activate and automatically send a panic alarm signal to the Security Operations Center, who in turn, will immediately notify the law enforcement agency having jurisdiction for response once the emergency has been verified. Audible/Visual devices will be strategically located in each facility to alert staff of a situation requiring immediate attention.
    a. Main property entrance gate(s) SOC.
2. Holdup alarm devices will be installed in the following areas that will activate and automatically send a panic alarm signal to the central station, who in turn, will immediately notify the law enforcement agency having jurisdiction for response, to signal a robbery in progress;
    a. Main property entrance gate(s)
    b. Dispensary
    c. SOC

Lighting

- ✓ The lighting at all the exterior doors and walk areas, around the parking lots and grounds and at the fence and gate will meet or exceed the requirements for Security Lighting.
- ✓ Infrared illumination devices will be deployed in certain areas to enhance the security surveillance of the property.
- ✓ Utilization of motion sensor lights to be implemented.

Patrol

COACHILLIN' will provide continuous patrol of the facility perimeter as well as all roadways throughout the property. Patrols will be staggered to avoid a predictable routine and all patrol personnel will be in constant communication with the Security Operations Center. Night vision equipment will be utilized for patrol during evening hours as needed.

COACHILLIN' security force personnel and all security vendors / contractors will wear uniforms that clearly identify their security role. Uniforms will be distinct from City and County law enforcement personnel to ensure clear identification of security personnel and law enforcement.

Perimeter Fencing

The cultivation facility grounds will be surrounded by a secure perimeter block wall and/or fence. The fence will be 8'-10' high and will be constructed of anti-climb and anti-cut. The fencing will be buried at least 1 foot below the ground. Alternative is the 8'-10' high block wall.

Facility Entrance

An overhead track gate with an electric slide gate operator and/or anti-crash barrier gate arm operator will be controlled specifically by the Security Force Officer at the COACHILLIN' ECP, and will be used for vehicle entrance and exit. COACHILLIN' is also investigating the potential use of security bollards at the point of ingress / egress to the facility. The use of delta barriers is also being considered.

Signage

Signage will be posted all along the perimeter fence line and at the entrance gate announcing "No Trespassing- Private Property" along with the appropriate terminology for video surveillance and armed Security Forces on duty.

INFORMATION MANAGEMENT

Coachillin operators responsible for the security of all marijuana items on the licensed premises, including providing adequate safeguards against theft or diversion of marijuana items and records that are required to be kept.

Cybersecurity

The Company recognizes the cyber threats that may impact the facility. The company will take precautions to ensure consumer privacy, protection of sensitive financial records, and minimize the potential of unauthorized access or intrusion.

As appropriate, the facility's network infrastructure will be encrypted and password protected.

Only authorized personnel who have been trained in secure records management procedures will have access to customer data. Users will have role-based authentication, and sharing of logins is prohibited. Software will require security measures such as password lockouts, login timeouts, use of strong passwords, periodic required password changes, and ability for administrators to disable users.

Records Retention

All electronic records will be stored both onsite in short-term storage, and off-site, in long term backup storage.

Onsite back-up records storage may include electronic media that is backed up on a daily basis on a secure server. The secure server will be physically located in a secure room on the premises. Offsite secure data storage will be managed by a third-party data storage provider. In general, Onsite backup storage will include at least 30 days of historical data. Remote data storage will include all data records that are at least 30 days and older, and will be stored in perpetuity. Data older than 4 years may be purged from storage.

All archived required records not stored electronically will be stored in a locked storage area.

Current records may be kept in a locked cupboard or desk outside the locked storage area during hours when the licensed business is open.

Sensitive files may be password protected, or stored in a password protected file storage system. No company files shall ever be stored in public internet spaces, including un-secured file storage sites. Emailing sensitive data files to anyone outside the company is strictly prohibited without the permission of the General Manager. Customer-specific transaction data and contact information, including email addresses, will not be shared with any third party without permission of the customer.