Divino Tessera, LLC

Security Plan

Commercial Cannabis Retail Storefront

Security Plan

March 2021

Mission Statement

Ollivier Security's mission is to successfully coordinate the security and protection of Divino Tessera's Cannabis Retail Storefront personnel and facilities, and function effectively across all aspects of the organization and the community it is a part of. Ollivier Security's success is measured by Divino Tessera's abilities to operate safely and securely, unconstrained by adversarial threats or theft of any kind. This Security Master Plan contains Ollivier Security's long and short-range strategy to meet and successfully execute that mission.

Executive Summary

Divino Tessera's Security Plan details all-encompassing security provisions from transportation to inbound distribution. The Security Plan provisions will comply with or exceed local laws and ordinances, California Prop 215 and SB 420, as well as the regulations promulgated under Article 5 as stated by The Bureau of Cannabis Control (sections 5042-5050), best practices from other regulated states and guidelines set by the federal government in the 2012 Cole Memorandum. Divino Tessera's 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 Divino Tessera's properties, Divino Tessera will implement a cannabis delivery security program to combat all known and potentially unknown threats. Divino Tessera has anticipated threats from every arena, including but not limited to physical, cyber, and procedural security for all facilities, vehicles and operations. Divino Tessera's program is designed to give every employee the responsibility of ensuring and working within a secure environment. Divino Tessera's 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.

The Security Plan provides for the long-range planning of physical security, technical security, and access control elements protecting Divino Tessera's facilities. It is the intent that the Security Plan is used as a guide to initiate the execution of design and construction of these physical and technical security projects. Construction must be integrated with the proper implementation of Standard Operating Procedures (SOP), Techniques Tactics and Procedures (TTPs), Contingency Operations and Plans (CONOPs), emergency action plans or other methodology for responding to incidents at the facility and while in transit.

There are several strategic and tactical considerations and assumptions that bear discussion to serve as a basic need and premise for this document. With its intended use and geographic area, the Divino Tessera facility has a complex security environment. Given the intrinsic value, the facility's missions must be sustained and remain protected 24 hours a day, seven days a week, 365 days a year. The main assumption is that there is always a certain amount of risk that is unavoidable and can only be reduced to a certain extent. These risks and subsequent constraints will drive defense in-depth and layered defense strategies outlined herein. Additionally, execution of this plan will require not only internal coordination with the Divino Tessera corporate structure, but external coordination and partnering with state and local government jurisdictions as well as stakeholders owning, occupying, or using space adjacent or near the facilities.

The application of this Security Plan is dedicated to the development of Divino Tessera's minimum standards and guidelines that designers, engineers, security professionals and/or Divino Tessera leadership can execute to maintain around-the-clock, 360-degree security posture of its facilities.

The minimum baseline security requirements for the facility is not to simply reiterate existing standards and requirements as set forth by the State of California, but to exceed those standards in every way as the responsibility to provide protection for Divino Tessera's people, facility, and assets is Divino Tessera's most paramount goal. In addition, the Security Plan provides the blueprint for integration of special design and security considerations for the facilities and vehicles with the decision-making process that focuses on detection, deterrence, delay where necessary, verification, response, mitigation, and recovery while protecting personnel and assets.

The overall goal is to prevent product diversion by both employees and customers, deter, detect, and delay when possible, intrusions of the facilities by an adversarial threat, through reliable security measures such as physical security patrols, perimeter fencing, sensors/automated detection systems, physical barriers (including but not limited to active, passive, visual, audible), video analytics, video surveillance, security lighting or other sensors. Intrusion detection must occur within ample time to allow for an immediate and proper response by the cognizant authorities.

As an example, the typical first layer of deterrence, detection, and response, will be accomplished with an integrated perimeter sensor/alarm system that instantly alerts Ollivier Security for appropriate response. Staff then both visually and audibly, acknowledges the receipt of the alarm, verifies the validity of the alarm through other sensors, and coordinates an effective response. The next course of action is dispatching the appropriate response within the shortest timeframe to mitigate the incident, secure an incident scene, prevent damage to the facility or vehicle and when required and possible - plan recovery operations. Throughout the response, the SOC will continue to monitor and maintain 360-degree situational awareness and vigilance over their respective facility and assets to be prepared for additional threats, and plan for possible worst-case scenarios.

Elements to be used include sensor systems, ECPs, access controls (vehicle and pedestrian), video surveillance systems and other technology necessary to ensure a posture of seamless, unobtrusive operations to project deterrence, provide proactive readiness, and agile capabilities, and allow for the conduct of appropriate security operations at the facilities. Rapid detection and assessment of intruders, multi-layered protections, and defense in-depth, will be our standard.

The overarching concept for security ensures that the SOC will have situational awareness of all security sensors, barriers, response, and actions taken at their facility. This Security Plan complements the SOC mission, which includes the command-and-control spectrum of security; from detection, assessment, and response to documentation and lessons learned.

Ollivier Security Team: Experience & Leadership

Divino Tessera will be retaining Ollivier Security as its security advisors upon license approval by the City of Los Angeles. Ollivier Security provides comprehensive security solutions specifically for the legal cannabis industry and will be addressing all security-related or effected aspects of Divino Tessera's facilities. Ollivier Security specializes in creating all-encompassing Security Plans which integrate technology, personnel, policy, and procedure.

Once Divino Tessera is awarded its license, Ollivier Security will provide complete turn-key execution, operation, management, testing, and maintenance for all security equipment and personnel within Divino Tessera's facilities. Ollivier Security will also be providing cost-effective security systems, enterprise operations and management solutions for Divino Tessera's facilities.

Ollivier Security is not just a security company, but a Systems Integrator and its competitive advantage over security companies currently providing Security Plans for this industry, is its blended approach to solutions. This approach to security comes from Ollivier Security's management and experience in the cannabis industry.

Ollivier (pronounced Oh-liv'-eeay) integrates physical security and information security. It designs and installs electronic security systems, including:

- Video surveillance with analytics
- Access control with integration of video surveillance, intrusion detection and other systems
- Visitor management
- Intercom IP and analog intercom (a.k.a. two-way emergency communication)
- Mass notification systems
- Asset Tracking (i.e. State RFID Track and Trace Tags)
- Digital evidence management and gathering

Ollivier Security's leadership takes the form of master Security Plans, engineering of security systems, governance over security operations, annual assessments and collaboration between physical security and information technology personnel. Ollivier's system engineers are computer science and electrical engineering graduates, specializing in network and database architectures. Each has extensive certifications, training and experience in security technology. Ollivier is a Certified Small Business Enterprise with the State of California and a preferred vendor for USC and Kaiser, two of the largest and most complex security systems in Southern California.

Business Statistics and Licensing:

- Market: Southern California
- Industry Sectors: Commercial; Local Government; Law Enforcement; Commercial Cannabis
- Founded: 1987 (Incorporated June 22, 1990)
- Corporate Headquarters: 8726 Sepulveda Blvd, D311, Los Angeles, CA 90045
- Satellite Locations: Santa Clarita, CA; Hawthorne, CA and City of Industry, CA
- California Contractor's License: C-7, C-10 #616791
- Bureau of Security and Investigative Services License Alarm Company Operator 7694

Ollivier Security Team – Cannabis Industry Experience

Safe Port Cannabis Dispensary – Retail - Port Hueneme

Ollivier Corporation installed and commissioned the Access Control, Digital Video Recording and Intrusion Detection Systems for Safe Port Cannabis. This project also involved meetings with the Police Chief of Port Hueneme to coordinate the installation of a full featured remote viewing iOS app in the 911 police dispatch center of the city. The remote viewing capability allows a police department dispatcher to view inside the dispensary at any time. The remote viewing app is used for alarm verification allowing a dispatcher to give the first responders information about what is going on inside the business. Ollivier also provides Intrusion Alarm monitoring through a U.L. listed Central Station and hostes the Brivo Access Control headend software.

Aureus – Cannabis CO2 Extraction, Distribution – Cost Mesa

Ollivier Corporation redesigned, installed and commissioned the Access Control, Digital Video Recording and Intrusion Detection Systems for Aureus. This project was unique in that the system design was begun by the now defunct security company CannaGuard. Ollivier was engaged to redesign the system once CannaGuard shut its doors leaving the client without support midway through the local municipal application and permitting process. An Ollivier representative was called in to represent the client at the planning commission meeting resulting in approval of Aureus' Conditional Use Permit (CUP)

Silo Inc. – Transportation, Distribution, Secure Storage and Quality Assurance – Southern California

Ollivier has provided security design, implementation and ongoing support at multiple locations for Silo Inc. throughout California, enabling this Distributorto grow and succeed safely, providing the community with jobs and ensuring safety in transportation and

Additional Cannabis Clients in California at various stages of progress to become fully operational:

The Bake Shop LA, LLC – Los Angeles – Retail, Distribution, Grow Facility, The Ollivier Security Plan has been approved by the state and is in review with the city of Los Angeles

VRX Labs – Long Beach – Laboratory Services - The Ollivier Security Plan has been approved by the state for three individual testing labs.

Plus Products – Adelanto – Edible Manufacturing - Ollivier has provided a system redesign/recovery plan for the existing failed in place security systems to return the client to state compliance.

Potology, LLC – Costa Mesa – Distribution and Manufacturing – Ollivier is in the process of providing a redesign and installing Access Control, Digital Video Recording and Intrusion Detection systems.

Background

This Security Plan shall be treated as a living document and shall never be considered complete. This document establishes a security program for the Divino Tessera facilities based on their existing operation plan. It is required however, that this document be modified at the appropriate time following an operational change. In most cases, the document should be modified immediately after the decision to modify an element contained herein. In addition, upon start-up of business operations within Divino Tessera facilities, this document shall be immediately evaluated and modified where appropriate. Throughout the life of this document, it shall be, at a minimum, reviewed, and revised as needed, on a bi-annual basis. Revision shall be the product of lessons learned, real-world conditions, specific threats, operational additions and subtractions, and operational need. No less than every other year, it shall be the responsibility of Divino Tessera to form a Security Plan review working group, consisting of stakeholders from all departments with Divino Tessera, with the intention of analyzing and updating the Security Plan to reflect the sum of knowledge and lessons learned from the last operating period.

Cannabis Security in Sun Valley, County of Los Angeles

Divino Tessera is located in Sun Valley, within the County of Los Angeles, with a population of 77,748. Cannabis Retail is considered a high-risk business, similar to bars, jewelry stores, or convenience stores. High-risk businesses are defined as those that have highly valuable products and a large sum of cash that may cause temptation for criminals or promote crime. However, despite being high-risk, cannabis retail storefronts differ greatly from bars or pawn shops in how they are built, managed, and secured to deter criminal activity. Businesses in the cannabis industry are tightly regulated and owners must abide by specific regulations. In regard to security, Divino Tessera must follow this Security Plan, along with the Standard Operating Procedures for Security located in Appendix A. prove worth and intent before they are licensed and approved to open. These documents are designed to reduce crime, theft, diversion and ensure the protection of the community and its employees and property.

Current Sun Valley Crime Statistics:

Violent Crimes

Calculated annually per 100,000 residents		National
Assault	**279.8**	282.7
Murder	**1.2**	6.1
Rape	—	40.7
Robbery	**123.3**	135.5

Property Crimes

Calculated annually per 100,000 residents		National
Burglary	**569.5**	500.1
Theft	**803.6**	2,042.8
Motor Vehicle Theft	**541.1**	284

(source: https://hoban.law/2019/10/cannabis-communities-crime-stats/)

Security Objectives

The objective of the Security Plan is to create the necessary protective elements for Divino Tessera facilities' critical infrastructure and key resources. The objectives of the Security Plan are identified below:

- Establish an entity within Divino Tessera responsible for all aspects of Physical Security within Divino Tessera facilities and in transport.
- Establish a basis for the design and implementation of facility and mobile security systems.
- Ensure that the integration of technologies and programs form a protective envelope around the facilities and safeguard mobile security.
- Establish and define the public areas, exterior facilities' areas, and the interior areas' systems and/or threat mitigation methodologies that provide deterrence and detection capabilities allowing emergency response forces to respond efficiently.
- Establish a path forward that incorporates new knowledge, evolving technologies, and lessons learned into the design and execution of future upgrades, systems, integrations, policies, and procedures that provide an even more timely and accurate detection of threats and subsequent responses.
- Ensure the testing, validation, commissioning, acceptance and exercise of deployed security systems to validate the security enhancement processes and protocols to include the implementation of Quality Assurance (QA) for integration activities.
- Establish a full spectrum of policies and procedures for the operation, training, execution, and sustainment of the Divino Tessera's security program and all systems and personnel contained therein.

Cyber Security

The protection of Divino Tessera IT assets and other systems residing on the Divino Tessera network present a unique challenge. In response, a Divino Tessera IT department shall be founded, and Cyber Security shall be one of the department's primary responsibilities. The Security Plan addresses cyber security as all security systems that depend upon cyber assets must be protected against tampering, intrusion, disruption or damage, both physically and through cyberspace. Cyber security will be an integral part of any sensor suite, IDS, video surveillance or other electronic systems being employed to address security at the facility. All cyber security systems should allow data transfer over a protected network into the SOC alarm system. The physical protection of the cyber assets will be handled in the same manner as other parts of the physical security envelope, while protection of the cyberspace will fall under the responsibility of the Divino Tessera IT/Cyber Security department.

While IT infrastructure, systems, and equipment shall be the responsibility of the Divino Tessera IT department, specific systems deployed within or in support of operations pertinent to Divino Tessera, not belonging to or deployed directly by Divino Tessera IT, shall have a responsible party from the Divino Tessera unit funding and/or requiring the deployment of the system. These responsible parties shall be designated as "System Owners".

Once a system enters the production environment, patching, sustainment, and risk mitigation becomes the responsibility of Divino Tessera IT. In cases where specialized skills are required to sustain the system, the System Owner shall enter into a contract with a 3rd party vendor for sustainment expertise and assistance. A memorandum of understanding (MOU) shall be authored and executed between Divino Tessera IT and the System Owner detailing roles and responsibilities with the system.

Divino Tessera IT shall maintain a list of System Owners and shall provide a list of proposed patches to the System Owner, no less than five business days prior, for patches Divino Tessera IT intends to apply to their respective systems. Should the system owner advise Divino Tessera IT that a particular patch would have adverse effects on their system, Divino Tessera IT shall assess the impact and determine if a waiver is needed.

Divino Tessera IT shall use firewall equipment that utilizes intrusion detection technologies to prevent unauthorized penetration of Divino Tessera systems, networks, and equipment. Any IT traffic traversing non-Divino Tessera controlled networks must pass through this firewall before entering a Divino Tessera network. This includes VPN and encrypted traffic originating from another Divino Tessera facility utilizing the internet or other non-Divino Tessera controlled infrastructure.

Divino Tessera IT shall conduct standardized IT penetration testing on all systems on a Divino Tessera network no less than weekly. Any system routinely utilizing external resources like the internet, shall be tested twice weekly, and acceptable service level agreements (SLA) will be executed with regard to security and availability, on any cloud storage or external IT resources utilized by any system supporting Divino Tessera or its operations.

Integrated Security Master Plan – Defense in Depth

The concept of a Defense in Depth, also known as the "Layers of Security", is an important element to any security posture, and is a critical component for the protection of the Divino Tessera facility. Shown conceptually in Figure 2 below, the entrance to Divino Tessera facility shall be the second layer of defense and the third layer shall be the inside of the building itself (i.e. vault or secure room access). This is a standard methodology where any installation has control of the entire physical property.

Protecting and defending the Divino Tessera facilities is unlike most applications whereby there are unique challenges with regards to meeting its protective and operational mission while having minimum impact on the public.

Public/Common Area

Beyond the facility's property boundary is called the Public/Common Area. This outer layer currently does not have a contiguous fence line and does not represent a clear means to detect, deter, delay or deny intruders or aggressors. These are potential areas where personnel and vehicles have unfettered access, potentially have a public right to temporary occupation, and cannot be challenged by Divino Tessera personnel. As required, Divino Tessera personnel shall monitor these zones by foot and SOC surveillance to proactively project deterrence and intercept threats as needed. While it is unlikely that detection at the outermost exterior perimeter will prevent a successful breach onto the property, early warning and detection at this layer is critical and will provide the ability to implement an appropriate response and stop an attack before any damage to the facility or its occupants can occur.

Exterior Facility Property

The next existing layer of security is known as the Exterior Facility Property and consists of the parking lot belonging to the facility and neighboring businesses. Once a vehicle or pedestrian enters this area (either via the entry point or surreptitiously), the exterior cameras and the VMS, utilizing advanced video analytics, alert the SOC of their presence. This allows another means of detection and advance warning for Security personnel to intercede a threat ahead of adverse action. If the entering vehicle is permitted, and in possession of the required documentation and permit, vehicles may park in designated spots only.

Facility Interior

All entrances to the facility interior will be secured with intrusion sensors, preventing forced entry, along with access control devices. According to assigned access rights, a person can enter the facility with an access card and their PIN. All employees will be asked to provide a four-digit access PIN as well as a four-digit panic/duress PIN. Should the employee attempt access with the panic/duress PIN, the opening of the entry will follow the employee's normal access rights.

However, when the panic/duress PIN is used, a silent alarm is transmitted to both the Divino Tessera alarm company, Emergency24, and the Contra Costa County authorities where appropriate. Within the facility interior, intrusion sensors, video surveillance and door locking devices secure certain interior spaces from common access. Therefore, inside the facility, Security will maintain patrols in common

areas, inspect credentials and have the ability to determine if personnel are in an unauthorized area. If contingencies arise, Security can restrict movement by segmenting the facility with appropriate door closures.

Vehicle Access Control

The parking management strategy for the facility serves several goals:

- Prioritizes a potentially scarce resource
- Establishes policies to comply with regulations such as the Americans with Disabilities Act (ADA)
- Contributes to a secure environment for employees and staff

Vehicle and Personnel Requirements for Passing Between Zones

The following are minimum requirements for passing from the Public Area into the Facility Exterior Area:

1. Visual screening of the vehicle when possible. Presentation of proper personal identification card by employees. Vehicle and/or passengers will have passed the screening with no issues. Presence of proper vehicle identification element (parking permit or other identifying trait as determined by Parking Management) linking the vehicle to the authorized person(s).
2. Visitor access requests shall be made no less than 24 hours prior to the visit and shall be made and authorized via a web page existing on the Divino Tessera internal network. An authorization form shall be produced by the system and it is the sponsor's responsibility to provide a copy to the visitor prior to the visit. Ollivier Security personnel assigned to manage visitor access will sign the visitor into the California State compliant visitor tracking log. The visitor log will be maintained by the Facility Coordinator and reviewed for accuracy and compliance by the manager daily. The visitor log will be accessible at all times for inspection by the California State Department and County.

Deliveries

While it is not required that deliveries be pre-authorized in the visitor management web page, they should be announced to manager each day. Should an unannounced delivery arrive at the facility, Ollivier Security Officer will contact the appropriate Divino Tessera management personnel for approval to enter. All deliveries will be handled through the designated delivery entrance and be subject to search by a Security Officer. Signs clearly directing delivery vehicles to the entrance shall be posted.

Once cleared by a Security Officer, delivery vehicles will immediately pull/back-up into the loading dock. All deliveries shall be received under the supervision of a Security Officer by Divino Tessera Inventory Specialists.

Perimeter Doors

Protecting ingress and egress is of paramount importance in maintaining an interior layer of defense. Additionally, doors may represent life safety code required egress points, security only devices, exit only device, or other classification.

All interior and exterior doors have been identified and classified and appropriate security measures have been planned. At a minimum, if any door other is propped open or is left in an open position for more than fifteen (15) seconds, an alert must be sent to the SOC and appropriate actions taken by Security Officer to secure the door if required. There are doors within the Divino Tessera facility that require the ability to be in the open position for several minutes and include roll-up and other delivery area doors. In these cases, Security Officer shall have the ability to bypass these doors and shall only do so when an authorized individual makes a request that this is done. This request can be in person or on the phone and does not need to be a formal request. Divino Tessera requires that all perimeter access points, including any man-passable opening, be adequately protected to prevent unauthorized access to the facilities. Any life safety classified door shall meet all of the National Fire Protection Agency (NFPA) life safety requirements and be equipped with standard panic hardware that allows for immediate egress upon activation. Egress shall never be hindered in anyway on a door classified as a life safety door. have. Similarly, all security classified doors shall have the minimum criteria:

Audible Alarms

If a door is opened without proper authorization (breaking, bypassing the access control device, exiting in an unauthorized manner) an audible alarm sound is made in the operations area with the alarm identifying the door location. This audible sound will remain until acknowledged by Security Staff.

Map Display

A map is displayed of the area that shows the door location and number that's in alarm. The map display shall show the door in red.

Access Control

All elements of the ACS system shall follow the below requirements:

- Primary communication to the head-end shall be accomplished via standard IT network communication protocols.
- All access control doors must send the "forced door" alarm condition to the SOC and monitoring alarm company, Emergency24, should the door be forced opened one (1) inch or more without proper ingress/egress procedures being followed.
- All access control doors shall be equipped with keypad and prox-card technologies. The system shall be configured to allow authorized personnel entry upon producing a valid four-digit PIN and a valid prox-card.
- All access control doors shall be equipped with high-security, non- residential, ANSI grade one (1) hardware.
- NFPA code shall apply to all access control doors within, and on the perimeter of, the facility. As such, life safety compliant exit devices shall be installed on, or within, within three (3) feet of every door.
- All access doors shall be equipped with high security balanced magnetic (BMS) door switches that employ an independent tamper circuit.
- All locking hardware shall employ manufacturer specified anti-picking technology.

- Should any component of the ACS fail, an alert is to be immediately sent to the SOC and alarm company, Emergency24, within 90 seconds. Should a failure last, or be anticipated to last, longer than 24 hours, Divino Tessera shall consider compensatory measures and alert Divino Tessera Operations Management as soon as possible.
- Access cards and PIN shall not be shared and must remain in the possession of the employee to whom it was issued at all times.
- Employees must report any lost or stolen access card to their manager within 24 hours.
- ACS shall maintain, for no less than one-year, complete electronic access control records to include, but not limited to, access granted, access denied, and system modification by user.

Intrusion Detection Systems - Alarm

All elements of the IDS system shall follow the below requirements:

- Must be protected against tampering, and must alarm, if tampered, to the Divino Tessera alarm monitoring center, Emergency24, as well as back to Ollivier Security
- All facility perimeter walls shall be protected against intrusion by volumetric sensors.
- In addition to volumetric sensors, all vault walls and security safes shall be protected against intrusion via seismic detectors.
- All anti-space above ceilings and below the roof shall be protected from penetration via dual-tech or better volumetric sensors.
- In any case where wireless technologies are not used, all intrusion sensor circuits shall be supervised.
- If wireless technology is used for intrusion sensors, communication between the sensor and the panel shall employ 256-bit encryption or better.
- Any facility perimeter opening of 24 square inches or more (i.e. HVAC vents) shall be deemed man-passable and shall employ proper IDS to ensure exploitation does not occur.
- All alarms must report to the SOC and Divino Tessera alarm monitoring center within five (5) seconds of being activated.
- Alarm monitoring center shall contact the facility's SOC to determine if Redwood City Police, should be dispatched.
- They will dispatch the police if asked to by the SOC, the wrong code word is provided, or if there is no answer within the SOC.
- Should any component of the IDS fail, an alert is to be immediately sent to the SOC and alarm monitor within 90 seconds. Should a failure last, or be anticipated to last, longer than 24 hours, Divino Tessera shall consider compensatory measures as soon as possible.

Security Systems Battery Back-up

Divino Tessera shall enter into an SLA to provide emergency generators onsite within 24 hours of a continued power outage. All security systems shall be specified with no less than 24 hours of battery back-up in order to sustain critical nodes until emergency generators are brought onsite.

Facility Duress Alarms

The duress alarms provide an emergency response to a threat situation for key personnel and areas in the facility. Not only do the duress alarms alert the SOC to facilitate dispatch of Ollivier Security response, but also report to an offsite 3rd party alarm monitoring facility. The monitoring facility will first attempt contact with SOC via telephone, but will dispatch the police if asked to by the Security, the wrong code word is provided, or if there is no answer by Staff. Upon a duress alarm, the video surveillance system shall also automatically activate the closest video surveillance camera on the Security's camera call-up monitor.

Security officers also carry a portable radio with the ability to send a duress alarm to the SOC and offsite alarm monitoring facility and do not activate audible sound devices.

Diversion Prevention

All security systems, equipment and personnel will be designed and trained with not only safety and security in mind, but also from a diversion prevention perspective. Diversion, both internal and external is a major concern, all will always remain a focal point of Ollivier Security Security Team. It is crucial to ensure that no marijuana or marijuana related items leave the facility without the acknowledgement of both Divino Tessera Management and Security Security Team. Divino Tessera will work with Ollivier Security Total Security to establish policies and procedures specifically related to both employee and visitor diversion prevention measures, both proactive and reactive.

Work Station

The above identified system shall be available on computer-based work station in the Security area. This will allow anyone with assigned access to monitor and respond to any sector. All systems (VMS, ACS, and IDS) shall be fully integrated allowing for critical interface with the three systems on one workstation.

Video Surveillance with March Networks

Divino Tessera has engaged Ollivier Corporation to provide and install a March Networks 9000 Series digital video surveillance system with a minimum camera resolution of 1280 × 720 pixels. Cameras shall record continuously 24 hours per day and at a minimum of 15 frames per second (FPS). Ollivier, will design and provide a comprehensive Security Plan including a floorplan showing where each camera will be installed. The floorplan will be including a legend with the number of cameras and resolution of each camera. The plan will also include the manufacturers storage calculation used to determine the amount of storage required, with 25% overhead, to obtain the state mandated 90-day recording retention.

The surveillance-system storage device or the cameras shall be transmission control protocol (TCP) capable of being accessed through the internet. The physical media or storage device on which surveillance recordings are stored shall be secured in a manner to protect the recording from tampering or theft. Surveillance recordings shall be kept for a minimum of 90 days.

The video surveillance system shall at all times be able to effectively and clearly record images of the area under surveillance.

Each camera shall be permanently mounted and in a fixed location. Each camera shall be placed in a location that allows the camera to clearly record activity occurring within 20 feet of all points of entry and exit on the licensed premises and allows for the clear and certain identification of any person and activities in all areas required to be filmed as follows.

Areas that shall be recorded on the video surveillance system include the following. Areas where Cannabis goods are weighed, packed, stored, loaded, and unloaded for transportation, prepared, or moved within the licensed premises; Limited-access areas; Security rooms; Areas storing a surveillance-system storage device with at least one camera recording the access points to the secured surveillance recording area and entrances and exits to the licensed premises, which shall be recorded from both indoor and outdoor vantage points.

Licensed retailers and licensed microbusiness shall also record point-of-sale areas and areas where Cannabis goods are displayed for sale on the video surveillance system. At each point-of sale location, camera placement must allow for the recording of the facial features of any person purchasing or selling Cannabis goods, or any person in the retail area, with sufficient clarity to determine identity.

The March Networks digital video surveillance system shall be capable of integrating with an RFID system capable of reading the state issued RFID tags for automated track and trace Cannabis product information collection.

The video surveillance system shall be equipped with a failure notification system that provides notification to the Owner of any interruption or failure of the video surveillance system or video surveillance-system storage device.

The surveillance recordings shall be kept in a manner that allows the Bureau or local authority having jurisdiction to view and obtain copies of the recordings at the licensed premises immediately upon request.

March Networks Differentiators

March Network engineers are subject matter experts in risk assessment, regulation compliancy and design-build services for all aspects of security in the Cannabis market. At MJBizCon 2018 they exhibited the latest video solution for Cannabis operators. They have put together an outline of what their Cannabis video solution has to offer in each stage of the seed-to-sale process:

Video Surveillance

- The video surveillance system shall maintain as close to 360-degree. Coverage around the perimeter of the facility as possible. Total coverage of the exterior property shall be priority and obstructions to this coverage from trees, shrubs, vegetation, and other aesthetic implements shall be reviewed by Divino Tessera. Additionally, any project consisting of installations that may affect video coverage, either interior to the facility or exterior, shall be reviewed by Divino Tessera.
- Cameras shall be properly specified to operate in the lighting conditions of the use area. Auxiliary lighting may be used at Divino Tessera's discretion.
- Cameras shall be placed so that recorded images are captured within 20 feet of entry doors, where permitted by law, with the intent to provide quality facial images of everyone entering the facility.
- Cameras shall be placed within all limited or secure areas, where permitted by law, with the intent to provide quality facial images.
- Cameras shall be placed so that recorded images are captured in any area where a marijuana item is received, stored, weighed, packaged, or sold.
- A live camera feed from the dedicated camera for all access control doors will be automatically displayed on a monitor in the SOC should any alarm condition be activated for that door.
- Using a virtual button within the video interface, the SOC user shall have the ability to instantly to review 90 seconds prior to the initiation of the alarm, at thirty (30) frames per second (FPS) at 1080p.
- All cameras shall be capable of being viewed live (real-time) at 1080p or better and at 30 FPS.
- All cameras shall be recorded on digital network attached storage and archived at 1080p or better, 30 FPS, with a minimum of thirty (30) days storage capability.

- All cameras shall have the ability to produce two H.264 streams of video transmitted via standard IT network communication protocols. Each stream must be independently configurable.
- Using manufacturer specific software, all cameras shall be viewable (both live and archived) off-site, given the proper IT steps are followed and approved by the Divino Tessera IT department.
- A printer, capable of producing high-quality color photos, shall be connected to the system and be capable of being used to produce prints of still images within the video archive.
- Shall have dedicated backup power generation to provide coverage (UPS or emergency generation) capability for a minimum of 120 hours.
- Should any component of the video surveillance system fail, an alert is to be sent to the SOC within 90 seconds. Should a failure last, or be anticipated to last, longer than 24 hours, Divino Tessera shall consider compensatory measures as soon as possible.
- A log shall be maintained that includes, but is not limited to; The identities of the employee or employees responsible for monitoring the video surveillance system.
- The identity of the employee who removed the recording from the video surveillance system storage device and the time and date removed.
- The identity of the employee who destroyed any recording.

In Cultivation, Labs, Extraction & Distribution Facilities

- Obtain a visual record of assets as they pass through facility processing and testing
- Access to tracking automation through integrated video and RFID data
- The ability to rapidly search for missing inventory
- Reveal where more staff training is required
- Security Audits and Operation Audits
- Receive automated reports with video snapshots of different areas in the cultivation facility
- Regulation Compliancy

In Transit

- Obtain a visual record of assets as they travel from cultivation to dispensary
- Provide employee safety and assure product deliveries with GPS locations and video feed
- Integrate video with vehicle data to prove vehicles did not cross state lines
- Regulation Compliancy

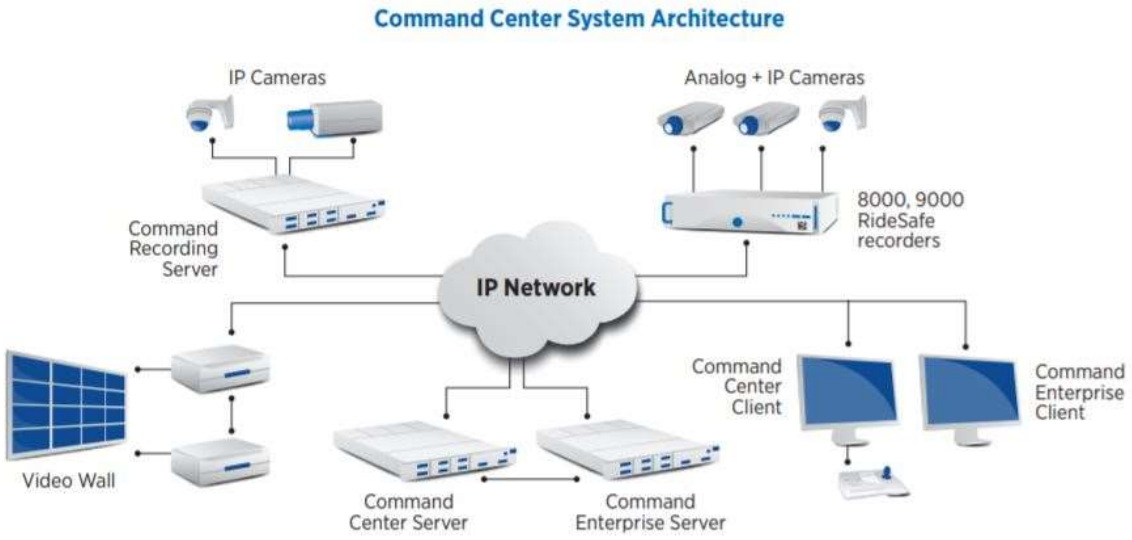
At the Dispensary

- Receive alerts triggered by suspect transactions through combined video and your POS data
- Run searches across multiple dispensary locations simultaneously
- Use video combined with analytics to track how long customers wait in line

9000 Series Digital Video Recorders

- Track which customers left the dispensary without making a purchase
- Track employee access to your product inventory
- Gauge the success of marketing or educational displays
- Regulation Compliancy

Typical Digital Video Recorder Topology



Armored Vehicle Daily armored vehicle pickup of cash deposits ½ Page

Divino Tessera will contract with Silo Inc. 63738 Orr Way Palm Springs California 92262. Silo's transport and delivery service offers a fully compliant transportation service for Cannabis products and will be utilized for both Cannabis product transport and (daily cash pickups in separate vehicles). The service provides a real-time inventory system which allows for vendor-managed inventory and just-in-time delivery reducing costs and maximizing revenue. This system is fully compliant with the state Track and Trace Cannabis product tracking system.

Cash Pickup Process:

During a predetermined window of time each day during normal business hours, the armored service will park at a predetermined perimeter door and alert security of their presents via cellphone and exterior intercom. The armed transportation guard will enter the vestibule and the identity will be verified against a list of authorized guards distributed by the transport service before being allowed into

the limited access area. The guard will then be sign in on the visitors' log and then be escorted to the cash counting room and retrieve a sealed deposit package for transport to the Owner's banking service. The transport guard will be escorted out of the limited access area and through the same route as entry.

Operational Consideration and Planned Procedures

Security Systems Testing and Sustainment

All electronic alarms shall be tested by Divino Tessera monthly.

- Ollivier Security Officer shall inform the 3rd party monitoring station that testing is being conducted.
- While watching the SOC alarm monitor, a Security officer will systematically activate all alarms, excluding tampers.
- Ollivier Security Officer shall document the status of each alarm and follow the reporting procedure should they encounter any failures or abnormal behavior from the system.
- All electronic systems and hardware shall be tested and repaired as needed by a qualified security systems vendor, no less than yearly. Divino Tessera shall maintain these records indefinitely.

Protection of Special Assets

All cash will be stored in the Modular Walk-In Vault (see photo below). The protection of this Walk-In Vault and safes are key and the following minimum specifications shall be met.

- A fully functional IDS system will be installed to include dual-tech or better volumetric sensors to detect any unauthorized presence in the room when secured.
- Seismic or equivalent sensors to detect any attempt to breach.
- True safe walls, no gaps, opening, or windows.
- Shall have a single point of entry.
- The door and frame shall be rated for thirty (30) man-minutes against surreptitious entry, ten (10) man-minutes against forced entry, twenty (20) man-hours against lock manipulation, and twenty (20) man-hours against radiological techniques.
- The Modular Walk In Vault shall be 2300° Ceramic Fire Blanket coated and be fire resistant up to one (1) hour.
- Point of entry shall be protected by a balanced magnetic switch (BMS) and must be controlled by electronic lock.
- The Modular Safe Room Vault shall be securely bolted to the concrete floor conforming to the manufacturer's recommendations.
- The Modular Safe Room Vault shall employ seismic or equivalent sensors to detect tampering.
- All sensors and electronics shall conform to the alerting standards as set forth in section 3.
- The vault shall be configured as a separate zone on the IDS.
- Under no circumstances may the Modular Walk In Vault be left open or disarmed.

Response Plans

Alarm response

Any alarm condition from any of the IDS sensors will require dispatch of Ollivier Security Officer to investigate the cause. An alarm can only be classified into one of three categories and requires Ollivier Security Officer to investigate and attempt to determine the cause and review the associated pre-alarm video (no less than 30 seconds prior to the alarm), and attempt to observe the cause, if any. The three alarm categories are as follows;

- False Alarm – Should an alarm be determined by Ollivier Security Officer to have no detectable cause; the alarm shall be categorized as false (system malfunction). Ollivier Security Officer shall then log the alarm status and provide the monitoring center with the appropriate instructions if applicable. This shall be reported to Divino Tessera's management via the procedure

- Nuisance Alarm – Should Ollivier Security Officer determine the cause to be tenant error, natural event (wind, wildlife, etc.) or other authorized activity, the alarm shall be categorized as a nuisance alarm. Ollivier Security Officer shall then log the alarm status and provide the monitoring center with the appropriate instructions if applicable. This shall be reported Divino Tessera management.

- Real Alarm – Should the alarm be caused by unauthorized, threat related, or otherwise adversarial activity, an appropriate security force related response is required. In addition, while maintaining a heightened state of security awareness of the rest of the facility utilizing the security tools at their disposal, Ollivier Security Officer shall contact the Redwood City Police, by dialing 911. Emergency24, the 3rd party monitoring company, will attempt to contact Ollivier Security. However, should Ollivier Security Officer become aware of a real alarm, they should in no case wait for Emergency 24 to call and should instead immediately contact the Police by dialing 911.

System issues

The following are the procedures that shall be executed for false alarms, nuisance alarms, and other abnormal system performance as detected by Divino Tessera:

- False alarms – Any alarm categized as "False" by Ollivier Security Officer shall be reported to the Divino Tessera Security Manager via email. The email shall have a subject line of "False Alarm Received – date XX/XX/XXXX, time 00:00:00". Within the body of the email, Ollivier Security Officer shall include the details of the response, the name of Ollivier Security Officer that physically responded, any pertinent details reported by that Officer, and any important observation or details the SOC Operator feels relevant.

- Nuisance Alarms – Any alarm categorized as “Nuisance” by Ollivier Security Officer shall be reported to the Divino Tessera Security Manager via email. The email shall have a subject line of “Nuisance Alarm Received – date XX/XX/XXXX, time 00:00:00”. Within the body of the email, Ollivier Security Officer shall include the details of the response, the name of Ollivier Security Officer that physically responded, any pertinent details reported by that Officer, the perceived cause of the nuisance alarm, and any important observation or details Ollivier Security Officer feels relevant.

- Equipment failure or abnormal operation – Should Ollivier Security Officer observe any offline messages reported from the Security Work Station, offline camera(s), malfunctioning cameras, inability to execute normal operations on any part ofthe systems, or any other perceived malfunctions of security related equipment or systems, email notification must be made immediately to Divino Tessera via email or telephone. Email shall include a subject line of “Malfunction – equipment name(s)”. The body of the email shall include the date and time the malfunction was observed, details of how the malfunction was observed (i.e. system reported, couldn’t see video on camera XXX, camera XXX would not respond to movement commands, etc.), potential impact operations.

3rd Party Monitoring company interaction

Ollivier Security communicate the status of the alarm (false, nuisance or real) and indicate to the monitoring company whether police, fire or ambulatory services are required. If any of the mentioned services are required, Ollivier Security Officer would provide as much detail as possible to aid the first responders.

Evacuation Action Plan

It is crucial to have a functional “Emergency action plan” that will facilitate employer and employee actions in the event of a workplace emergency. It is equally important to have designated individuals who will take charge and coordinate an organized response. Security Officer will be responsible for overseeing emergency events and shall be trained and capable of implementing all aspects of the “Emergency Action Plan.”

Evacuations

A facility may be required to evacuate due to both man-made and natural events. A disorganized evacuation can lead to panic, property damage or injury. These emergencies include - fires, explosions, floods, earthquakes, radiological and biological accidents, civil disturbances and workplace violence. It is important to establish a designated asset who maintains the authority to execute Divino Tessera’s planned procedure and is well versed on the established chain of command for all evacuation events. Security Officers will oversee all evacuation procedures and will be trained and capable of implementing the Evacuation Plan. The Evacuation Plan will incorporate procedures for the following:

- Maps and floor diagrams with arrows that designate the exit route assignments
- Procedures for assisting employees and visitors during an evacuation

- Designated employee procedures for shutting down critical operations before evacuating.
- Procedures for accounting for employees and visitors after an evacuation
- Procedures for coordinating with the appropriate first responders.

Initiating and Coordinating Police, Fire and Rescue, and Ambulance

Relationships with the local police force will be established via the designated Security Staff Liaison. The police department will have a direct phone number to contact the onsite Security Staff should they need to communicate quickly.

- Police: All Security Officers will receive specific instructions for requesting police assistance. All Security Officers will understand how to assess and properly relay all "Need to know" information when calling "911." Security Officers will utilize SOC and our third-party alarm monitoring company, Emergency24, to identify the area of the disturbance.
- Fire and Rescue: All Security Officers will receive specific instructions for requesting Fire and Rescue assistance. All Security Officers should always be aware of potential fire hazards and pay special attention to higher risk areas. During patrols Security Officers should inspect fire extinguishers and well as look for any potential hazards such as lose wires or flammable material risks.

  In the event of a fire all Security Officers will assist in contacting "911" and communicating all necessary details to the emergency responders. Security Officers will also be responsible for assisting in the evacuation procedures.

- Ambulance: All Security Officers will receive specific instructions for requesting Ambulatory assistance. All Security Officers will understand how to assess and properly relay all "Need to know" information when calling "911." Security Officers will assist in directing EMS personnel on to the property and directly to the area of the emergency.

First aid and triage

All Security personnel will be certified in First Aid and CPR. Additionally, all Security personnel will be responsible for the following first aid duties:

- Assessing the situation
- Calling 911
- Providing basic medical attention until emergency responders arrive
- Communicating and updating emergency personnel with crucial information such as specific location, real time situation updates etc.

Recordkeeping

It is the responsibility of Ollivier Security Officer to record in an excel log sheet (developed by Divino Tessera) all events of the evening to include;

- Arrival for duty
- Duty relief of all Security personnel to include breaks and lunch
- All alarm events and resolution
- Any reported conditions (i.e. Camera XXX malfunctioned at XX:XX:XX and was reported via email to Security Staff
- Patrols
- Dispatches
- Any other security related activity

Credential Issuance and Facility Access

No one under the age of 21 will be allowed to enter a Divino Tessera facility and therefore will not be issued and Divino Tessera security credential or access rights.

Divino Tessera will be responsible for the issuance of access credentials and the addition of access privileges to those credentials. Creation of the credentials shall be a function of the access control system and shall be done on a proximity enabled access card.

Employees will be required to successfully pass a background check before engaging in work at the Divino Tessera facility. Once favorable results of these background investigations are complete, security credentials will be forwarded to Divino Tessera HR for issuance to the employee. These credentials alone will not allow access to the facility or any other security doors within the facility.

Once cleared from HR, an employee's division head must send a request to Divino Tessera requesting appropriate access to only the access control doors within the facility required for the employee's assigned duties. Email requests from division heads and their designees shall be accepted and an appointment to enroll in the facilities ACS shall be scheduled with the employee within one (1) business day. Requested access will be granted during the enrollment process and will be effective immediately. The employee must bring the issued security credential with them to the enrollment appointment. It is the responsibility of Divino Tessera to retain all records of access requests as well as all records prescribed herein from all electronic security systems. This information must be immediately available upon request by the state of California, it's designees, and any other governing body having the right and jurisdiction.

Visitors

No one under the age of 21 will be allowed to enter the facility.Visitors requests shall be made no less than 24 hours prior to the visit and shall be made and authorized via a web page existing on the Divino Tessera internal network. This request system shall be a feature included with the access control system and authorization, view-only access (Security Officers), request approval/denial authority, and request modification rights shall be at the discretion of Divino Tessera management and enforced by Divino Tessera. An authorization form shall be produced by the system and it is the sponsor's responsibility to provide a copy to the visitor prior to the visit. The visitor will be required to present this form to Ollivier Security Officer to gain access to the facilities.

The visitors host will instruct visitors to provide Ollivier Security Officer their name and a government issued ID. Ollivier Security Officer will compare the name given to the authorized visits (contained within the afore mentioned web page) for that day. If the visitor is on the list, their host will be contacted, and they may then enter the facility once their host reports to the waiting room to begin escort. The visitor's host is responsible for the actions of the visitor while in the Divino Tessera facility and the visitor must always be within visual contact and escorted (excluding the restroom). Any violations of Divino Tessera policy will be grounds for removal of the visitor immediately.

Physical Security Officers

California security officers are credentialed by the Bureau of Security and Investigative Services. They must hold these credentials unless they fall under exemption categories described in state statute.

A prospective security officer will need to be fingerprinted and criminal background checks are carried out by the California State Police and through the Federal criminal database. The applicant will provide a notarized release of information form. He or she will authorize California State Police to obtain information, as necessary, from various sources, including educational institutions, mental institutions, and credit reporting agencies.

Once approved, the individual will need to complete a training program. It will include "The power of arrest training course," (BPC Sections 7583.6 and 7583.8). 32 hours of instruction and will be taught by a certified instructor. Training is to be completed within 30 days of employment.

Registration is renewed annually, and the security officer will need to take an 8-hour refresher course.

A security guard must be commissioned to carry a firearm. A commissioned security officer must be free of felony convictions (unless a pardon was granted). Additionally, the individual cannot have committed acts which would result in revocation or suspension of a license issued by the California State Police.

The prospective commissioned guard will need training in each of the following content areas: weapons and safety, legal limitations of firearm use and marksmanship/range safety. The prospective armed guard should expect examination on each required topic. It will be necessary to qualify on the range. California requires a demonstration of safe handling and usage. There are many alternatives. The applicant may demonstrate that he or she has completed an appropriate course, test, or qualification. The instructor or provider does need to represent a reputable organization. An instructor may be qualified based on certification by the National Rifle Association or a police academy.

Divino Tessera has contracted security officers through a Ollivier Security Total Security Solutions a division of Security Resources and national security guard provider. Security Resources guarantees fully licensed, trained and insured security officers vetted by the state of California. In addition to the California minimum qualification requirements mentioned above, all security officers will meet or exceed the following additional qualification requirements set forth as per recommendation of Security Resources d/b/a Ollivier Security Total Security:

- Must be at least 21 years old and possess a high school diploma or General Ed. Certificate (GED)
- Must be U.S. Citizen
- Must fluently speak, read, comprehend and compose coherent written reports in English
- Must not use illegal drugs. Must submit to a pre-employment drug test
- Must have firearms experience
- Must have one of the following experience levels listed:
    - Three years armed security experience
    - Three years military experience
    - Completion of State certified Law Enforcement Education
    - Completion of a Police Officer's Standard Training Course
    - Possess good written communication skills

- Capable of verbal communication adequate for clearly understandable radio Transmissions Proficient in diversion tactics and capable of proactively identifying both internal and external diversion risk
- Perform duties requiring moderate to arduous physical exertion involving standing for prolonged periods, walking, running and climbing stairs or ladders.
- Demonstrate good customer relations and interaction skills
- Must be able to operate and work in multi-task environment
- Successfully complete an interview structured to evaluate general knowledge and abilities to perform security tasks to include decision-making abilities
- Ability to assess and evaluate situations effectively
- Ability to identify critical issues quickly and accurately
- Ability to contribute and participate in a team environment
- Proficient end-user lever skill set with electronic security measures
- Must be of sound mind and moral character, with no felony convictions or convictions for misdemeanors involving moral turpitude, domestic violence or work place violence
- Qualify with the authorized duty handgun by scoring a minimum of 80% accuracy within the prescribed time on the certified firearms course

Staffing Plan

Effective workforce planning entails having the right number of people with the right skills working in the right jobs at the right time. Security personnel staffing refers to the examination of the total duties to be performed within the scope of security and the placement of properly trained and qualified personnel to perform those duties.

Divino Tessera has contracted the services of Ollivier Security Total Security which will employ the proper considerations to identify required increases and decreases in staffing, and to identify technical, management, and/or support position skills needed to accomplish organizational functions and objectives.

As stated, this Security Plan will be implemented and reviewed no less than bi-annually. Ollivier Security will assist in identifying and updating training requirements and individual skills development for all security staff as well as the expected security procedures and processes within Divino Tessera. Clear and explicit delegations of authority and responsibility will be provided and documented at all levels.

Security Officer Positions, Duties and Schedules

All Security officers assigned to Divino Tessera Facility will play a crucial role in safeguarding life, property and critical space hardware at Divino Tessera. Divino Tessera Facility will operate from 8:00AM to 9:00PM, 7 days per week. During the hours in which Divino Tessera facility is operational there will be a minimum of 1 Security Staff member with the flexibility to add additional staff during times of need. During the hours where the facility is closed, premises shall be monitored via video and alarm systems monitored by our designated alarm company, Emergency24. The standard security position shall be as followed:

● Security Staff Deputy –

o This position is a roving post and the deputy duty will be based in the Security Room which houses the security and alarm monitoring equipment.

o The schedule is based on a 168 hour, 7-day work week.

o This post will be staffed during all hours of Facility hours of operation.

Scheduling

A key component to proper security staffing is to ensure that there are always sufficiently trained "Back-up" officers on hand in the event of a last-minute call out, vacation request, abrupt resignation or termination of an officer. The most effective way to ensure access to fully trained replacement officers is to employ 2 part-time Security Staff members with position flexibility. These individuals will maintain permanent weekly schedules at Divino Tessera at a reduced number of hours but will also serve as "Fill-In's" when open posts become available. These individuals will be just as qualified, trained and experienced in their security roles at Divino Tessera as the full-time officers. In the event of an open shift these individuals will be called upon to fill the post. Whenever possible, Fill-In officers will be utilized rather than holding over officers. Excessively long shifts can reduce the effectiveness of security officers and should be avoided if possible.

Additionally, Fill-In officers can serve as an immediate short or long-term replacement for full time officers. To ensure enough coverage in the event of an officer call-out or the temporary need for additional staffing, Ollivier Security Total Security will:

● Make certain at the time of hiring that all security officers understand that there will be times when their relieving officer may call-out last minute, and they will be required to continue holding post past the end of their shift. Ollivier Security Total Security will take immediate action to contact the off duty part-time officers to fill the post and relieve the held over security officer. If scheduled Security Staff is unavailable for their shift (with proper approval), Ollivier Security Security will contact all off-duty full time SO's with the opportunity for overtime work.

● Ollivier Security Security will adhere to all California mandated overtime laws and regulations relating to security officers working past their scheduled shifts.

● Employ 2 officers that have permanent "Part Time" Schedules

● PT SO A and PT SO B will be trained and fully capable of performing the job duties required for all security positions at Divino Tessera

Personnel Training
Given the integration of the custom electronic security system that will be deployed within the Divino Tessera facility, Ollivier Security Total Security will ensure that all Security personnel be trained on the proficient operations of the system prior to reporting to the facility. In addition, Security personnel must receive refresher training no less than once every year and whenever new technologies are deployed.

Equipment Specification/Minimum Standards

Safe
Safes shall be a Custom 2300 Degree Ceramic Coated 3/16th Reinforced Steel Wall Walk-In Vault measuring 20 x 8 x 7

Radios
Radios shall be Motorola XPR 7350e or equivalent

FIREARMS
Security Security Officers will purchase and carry personal handguns as their primary firearm. Security Security Officers shall ensure his/her weapon exceed the standards and/or requirements set forth below:

RANGE QUALIFICATIONS: Each Security Officer must qualify with a minimum 90% score with the actual handgun he/she desires to carry as his/her primary weapon.

REQUIRED ACCESSORIES: Each Security Officer will be required to purchase and maintain all duty equipment required to utilize their personal weapon as a primary firearm, including but not limited to; holsters from the authorized list, magazine pouches, magazines, etc.

ANNUAL INSPECTIONS: Each Security will submit their firearm for annual inspection.

APPROVED FIREARMS:
All firearms carried by Security must be on the authorized list of weapons. The Divino Tessera SGT will maintain an authorized firearms list that will be updated annually.

Primary weapons for uniformed carry shall have a barrel length of not less than 4, nor more than 5.5 inches. Weapons shall be black or silver in color or a combination of black and silver. Removable grip panels shall not be ornate in nature and shall be black, grey or brown in color. If the pistol is fitted with a thumb safety, it must be ambidextrous for left handed shooters.
● Glock, “safe action” type, semi-automatic pistol in 9mm parabellum, .40S&W or .45 ACP, to include Glock models 17, 17C, 19, 19C, 21, 21C, 22, 22C, 23, 23C, 34, 35, and 41

● Sig Sauer P226, P220 and P250 pistols in 9mm, .40S&W or .45 ACP with DAO (double action only), DA/SA (double action / single action) actions
● 1911 design pistol systems chambered in 9mm, .40S&W or .45ACP produced by Colt, Kimber, Springfield Armory, Smith & Wesson, Sig Arms, STI, or as approved by Ollivier Security supervisor.
● Springfield Armory XD and XDm pistols chambered in 9mm, .40S&W or .45ACP
● Smith and Wesson M&P pistols chambered in 9mm, .40S&W or .45ACP MINIMUM TRIGGER PULL: for all Glock weapons will be four and a half pounds.

Background Check

The Owner will perform several steps to determine the eligibility of a potential employee before hire. Each applicant shall be at least 21 years old and be required to submit fingerprints to the Department of Justice for a criminal background check and pass that process without any disqualifying events being reported. In addition to the background check the applicant will require potential applicants to submit to a personal credit check through one of the three credit bureau reporting agencies. Successful candidates who pass the background check and are hired will be issued an employee identification badge. The identification badge shall, at a minimum, include the licensee's "doing business as" name and license number, the employee's first name, an employee number exclusively assigned to that employee for identification purposes, and a color photograph of the employee that clearly shows the full front of the employee's face and that is at least 1 inch in width and 1.5 inches in height.

Workplace Safety: Each program will have a site-specific segment acclimating the employee to the workplace. Workplace specific training will help educate workers to predict, prevent, identify and stop possible common worksite hazards. This part of the overall safety program will identify site safety equipment such as fire extinguishers, eyewash station, spill kits, first aid kits, emergency communication devices, fire alarm pull stations, panic buttons, emergency shutoffs for public utilities and machinery and demonstrate the proper usage of each. Any hazardous materials on the premises will be identified and employees will be shown the location of the MSDS datasheets and the location of Hazardous Material Business Plan (HMBP) stored onsite. The employees will be trained on safe handling precautions and first-aid notes for exposure to any caustic substances or active ingredients commonly found in cannabis products for each hazardous material in the workplace. At least one employee will be California OSHA-30 trained.

Employee Safety Education
A personalized safety training program will be administered to each employee based on their job duties/requirements.

Managers Training: The fire alarm provider will provide management a "train the trainer" course on fire pull station activation, central station procedures, sprinkler shutoff valve and location of replacement sprinkler heads. Ollivier Corporation will provide management training on robbery protocol, burglary protocol. Olivier Corporation will provide training for management such that they will possess a firm

understanding of how the system works. This will include the ability to issue, alter, and revoke access privilege to any area, for any employee, at any time. Management will be instructed how to control the various features of the camera system. They will also provide the following instruction for the proper operation of each security system. This will entail how to view, record, archive video and will also demonstrate how to categorize events in the system, allowing for prioritization of alarms based on business rules. Finally, management will be made aware of how the security platform incorporates the alarm system, including instruction of the sequence of operations for given alarm events. Exact details of this sequence will be shown in final plans. The monitoring account will be set-up with Owner providing the necessary contact lists, passwords, instructions, etc. as are required to establish a monitoring agreement between Ollivier Corporation and the Owner. Should a report showing the authorized personnel with security clearance level credentials be requested, one can be easily provided.

Delivery Drivers: Any person employed by the Owner that will be expected to drive or deliver products will have a clean driving record and will successfully complete a California Department of Motor Vehicles Approved Defensive Driving Course. The Owner will require any employee engaged driving as part of their job duties to successfully complete an age-appropriate course administered online by https://www.defensivedriving.com/ prior to getting behind the wheel.

Machinery Operators: Any person employed by the Owner that will be expected to operate equipment or machinery will be required to successfully pass an OSHA 10 Course. OSHA 10 General Industry Training will help educate workers to predict, prevent, identify, and stop possible common worksite hazards.

Ongoing Safety Program: Management will conduct weekly safety meetings prepared by the following safety content provider: https://www.ehsinsight.com

Theft Reduction Measures

The Owner will reduce employee theft through a combination of loss prevention practices. These practices include the use of technology, policies, and procedures to deter employee theft.

Technology: The Owner has contracted with Ollivier Corporation to install a commercial grade electronic access control system to limit access to Cannabis products to only those individuals whose day-to-day duties require them access. The system also limits the employees' access to the building during regularly scheduled days and times of work duty. The building will be under video surveillance and the recordings will be stored for 90 days to deter theft. If retail sales are to be conducted in this location a point-of-sale loss prevention system manufactured by March Networks will be installed to associate video footage with all statistics of each transaction to be regularly audited to prevent shrinkage.

Policy: The applicant will fully adopt a policy to report any suspected theft to local authority's and to prosecute any theft of the law as a deterrent. This policy will be written into the employee handbook and displayed adjacent to other state mandated information on display in the breakroom.

Procedures: As a condition of employment employees will submit themselves and anything they are carrying into or out of the limited access area to a search by security personnel. Employees all be provided a locker outside of the limited access area to store personal belongings.

Cash Management Plan

The owner is anticipating and is planning for a high volume of cash transactions. Cash management will be a critical factor for the business with regards to employee safety, accounting accuracy, banking delays, provisions for secure cash storage and accommodations for physical cash transportation. The Cash Handling Procedure will be documented, and management will be responsible to train each employee on approved cash handling practices. Cash will be moved from the point of sale to cash counting, secure storage, then off premises to the owners banking institution via armored transport.

Point of Sale: The owner will use COVA Cannabis point of sale system that is compatible with Searchlight Digital Video Recording and Loss Prevention Solution designed by March Networks. The Digital Video Recorder will record each transaction at the cash wrap station. Cameras will be situated in a manner that will allow a closeup view of the cash wrap counter and will be recorded with an overlay of text generated from the point-of-sale system embedding the details of the transaction history in the video of the exchange of payment and product. This system will give management a much greater forensic audit capability than traditional point of sales systems alone. Ultraviolet counterfeit detectors and detecting pens will be utilized at the time of the initial transaction to minimize the risk of ingesting counterfeit currency.

Till Management: Every employee working the point of sale will be assigned a personal till that will have a preset starting cash amount as the shift begins. The till will be reconciled against the point-of-sale record at the beginning and end of every shift. Any discrepancies will be dealt with immediately. Regular cash drops will be performed upon reaching a preset cash threshold to maintain a minimal amount of cash on hand in the retail area at any given time. The Point-of-Sale system will be reconciled with the bank account daily.

Secure Storage: The cash processing will take place in a room with restricted access controlled by a Brivo access control system. All persons accessing the room will be registered with the date and time of access in the Brivo database. Access will only be given to management and individuals assigned cash handling rights during the hours of expected activity. The cash room will house a locked cabinet for till storage, a safe, counting tables, cash counting machines and cash supply storage for (deposit bags, associated forms etc.) The room will be outfitted with a situational awareness camera viewing the room as well as a camera focused on the cash counting area. No Cannabis products will be stored in the room at any time. The room will be used for till storage audits, reconciliation and cash counting for preparation of daily cash pick-up deposits.

Staff training: The staff will be trained on currency screening, point of sale usage, till reconciliation, cash drop procedure and responsibility and the escalation process for reconciliation discrepancies. Managers will be trained on all processes involving cash handling and analysis of the loss prevention trending data and advanced reporting capability of the Searchlight system.

Cash management is a critical process of the business and all systems and processes will conform to General Accounting Process (GAP).

Product Access Protocol

The Owner will put a system in place to ensure that only properly licensed and current agents, officers and employees have access to areas where Cannabis product are stored. This limited access measures will be implemented through the use of technology and procedures.

Technology: The Owner has engaged Ollivier Corporation to install a commercial grade Brivo electronic access control system with commercia grade electrified door hardware. This system will be installed on perimeter doors to the building, on the perimeter of the limited access areas and anywhere Cannabis products are stored outside of the schedule 1 vault. The access control will be programed to allow people possessing credentials to enter areas where their job duties require them to be and will be limited to the hours that individual is typically scheduled to be at work. The system will retain records of what day and time each door was entered by the individual for a minimum of seven years. Security personnel will have the ability to monitor all of the business operations surveillance cameras allowing them to ensure that only authorized people are in the limited access areas at any given time.

Procedures: All agents, officers, or other persons acting for or employed by an Owner shall display a laminated or plastic-coated identification badge. Employees will enter the business through the designated employee entrance that opens to a holding area outside the limited access area and will check in with security showing them their identification card for a positive identification prior to carding into the limited access area.

Delivery procedure

The delivery process will vary based on the layout of the building taking into consideration factors like vehicle approach, parking area while delivering and visibility to surroundings etc. The process will focus on participants safety, minimizing the impact of the transaction on surrounding businesses and accurate record keeping.

The core process will be as follows and include the details and safeguards listed. Deliveries will only be accepted during days and hours approved by the city and during daylight hours. Deliveries will be received using a predefined perimeter door. Any pedestrian doors will be equipped with a Brivo Card Access reader preventing entry by non-licensed individuals. If the premises has sufficient space for a vehicle to access via a rollup door, deliveries will be received once the vehicle is secured in the limited access area. Any adjoining doors to the delivery load/unload area will be equipped with a lamp/beacon that will illuminate while the outer rollup door is opened signifying to staff that the inner doors are to remain closed while the perimeter doors are open. The perimeter door will have both interior and exterior cameras. The door will be monitored 24 hours a day, any change in status of door will send signal to alert the system. The door will have to be disarmed by the site manager for the delivery and

rearmed once the delivery vehicle has left the premises and the door is secured. The managers unique disarming code will be communicated and to central station logged with a date and time stamp. The designated load/unload area will have a camera viewing the rear of the delivery vehicle. Cameras will be recording constantly with 15FPS being recorded onto the recording storage servers with a minimum of 90 days of archived video. A security guard and the site manager will accompany any incoming deliveries of Cannabis products. Should the delivery process require the vehicle driver to enter the limited access area the driver will be required to fill out the visitor/delivery log and the information verified against their driver's license. Any delivery drivers entering the premises will be escorted by a security guard for the duration they are in the limited access area. At the time of delivery any Cannabis products will be counted and reconciled against the bill of lading for accuracy. Cannabis products will be moved to a secure storage equipped with a Brivo card access reader. The door reader will be programmed so that only site managers and business Owners will have access to the room. All Cannabis product will be reconciled and secured prior to the perimeter vehicle access door being opened and the vehicle leaving the limited access area. The perimeter delivery door will then be rearmed. Any Cannabis products brought to the premises will be logged in the state reporting system Metric and will be tracked while onsite. The delivery procedures will be further refined to accommodate the floorplan and access limitations of the site. Deliveries of non-Cannabis products will follow the same process except for any requirement to log anything to the state reporting system.

The delivery process shall insure that any Cannabis products delivered to the site will be performed in a safe manner for delivery drivers and employees of the Owner. All steps to the process will be recorded either manually or through security automation. Any deliveries will be documented on multiple record keeping systems including Visitor Log, March Networks digital video recording, Brivo access control, Rapid Response UL listed monitoring station, delivery company's Bill of Lading, security daily activity report, and the state Track and Trace reporting system.

Security Guards

The Owner believes a strong visible security presence will provide a safer workplace for their employees and reduce the risk of criminal activity. The Owner will contract with White Rhino Group, Inc. Cannabis industry security experts. Security officers will be present during the business' hours of operation. There will be a minimum of one officer present during all hours of operation. All security officers will provide the Owner a copy of their license issued by the Bureau of Security and Investigative Services. The license expiration dates of the security staff will be tracked to ensure continuity eligible security officer coverage.

Security officers will perform the following duties for the Owner:

- Administer the employee check in and out process including searching articles brought in and out of the limited access area.
- Escort any vendors or visitors that are not staff members or agents of the Owner while in the limited access area.
- Monitor the premises with the aid of the alarm and video surveillance systems.
- Document daily activity and report on any security related incidents

Appendix A

Standard Operating Procedures for Cannabis Retail Storefront Security

GENERAL, OPERATIONAL, & FACILITY SECURITY

DBA places great importance on the safety and security of its employees, as well as the members of the surrounding community. DBA will contract with City approved security company, a local security firm that will be responsible for the business's 24-hour on-site security/protection.

1. Divino Tessera will, at all times, implement sufficient security measures to deter and prevent unauthorized entrance into areas containing cannabis or cannabis products and to deter and prevent the theft of cannabis or cannabis products at the commercial cannabis business. Except as may otherwise be determined by the City/State or any of their designees, these security measures shall include, but shall not be limited to, all of the following:

    a) Prevent non-employee individuals from remaining on the premises if they are not engaging onsite for business-related reasons.
    b) Limited-access areas accessible only to authorized Divino Tessera personnel.
    c) Except for cannabis goods on display or for sale in the retail area, all cannabis and cannabis products are stored in a secured and locked room with a safe/vault. All cannabis and cannabis products are kept in a manner as to prevent diversion, theft, and loss (detailed in the Security Plan).

2. Sensors shall be installed to detect entry and exit from all secure areas.

3. Panic buttons shall be installed in undisclosed locations throughout the facility.

4. A professionally installed, maintained, and monitored alarm system. Divino Tessera is open to the City's security alarm systems recommendations.

5. City approved security company will be on-site 24 hours a day.

6. City approved security company is licensed by the State of California Bureau of Security and Investigative Services.

7. While all exterior doors and doors leading to limited-access areas (including cash and product storage) are constantly secured by electronic locking mechanisms, they will additionally be outfitted with high-security, manual locking mechanisms to be implemented in the event of a power outage,

8. Divino Tessera will identify a Security staff member from City approved security company a designated security representative/liaison for the City of Los Angeles who will be reasonably available to meet with the City designees regarding any security related measures and/or operational issues. Divino Tessera shall notify the

City within twenty-four (24) hours of a change in designated security representative/liaison.

9. Intensive security measures will be implemented to ensure the safe and secure transport of currency and/or cannabis product into/out of the facility.

10. Divino Tessera will cooperate with the City whenever it makes a request, upon reasonable notice to the business, to inspect or audit the effectiveness of any security plan or any other procedures.

11. Divino Tessera will notify the City/State within twenty-four (24) hours after discovering any of the following:

    a) Significant discrepancies identified during inventory reconciliation
    b) Diversion, theft, loss, or any criminal activity involving the business
    c) The loss or unauthorized alteration of records
    d) Any other breach of security

See attached Security Plan for details on Security Procedures

AUTHORITY
Section 26013, Business and Professions Code.
Reference: Sections 26012 and 26070, Business and Professions Code.
Bureau of Cannabis Control Proposed Text of Regulations
(Title 16, Division 42, Chapter 1, Article 5—California Code of Regulations)
(Title 16, Division 42, Chapter 1, Article 3, §5033—California Code of Regulations).
Regulation No. 3.A.8(a) 5.A, 5.B, and 10.A—Ordinance 185344 Rules and Regulations for Cannabis Procedures.

LIMITED-ACCESS AREAS

1. In regard to non-employee or individuals who have not been authorized to enter the facility, the entire facility is considered a limited access area with an implementation of employee lockers provided by an approved vending partner.

2. Divino Tessera has established limited-access areas accessible only to authorized employees of the business.

3. All inventory stored on the licensed premises will be secured in a limited-access area.

4. Divino Tessera will not store cannabis goods outdoors.

5. Employee break rooms, changing facilities, and bathrooms will be separated from all storage areas

6. Each location where cannabis goods are stored must be separately licensed.

7. The following are considered limited-access areas within the facility:

a) All Track-and-Trace terminals
b) The Retail Area
c) Shipping/Receiving
d) The Break Room
e) Storage areas

8. The following are considered High Security Limited-Access Areas within the facility:

    a) The Security Room
    b) The Safe/Vault Room
    c) The Product/Cash Transfer Zone

9. The following staff members will be the only employees given full access to Limited-Access Areas:

    a) General Manager
    b) Manager
    c) Security staff

10. Divino Tessera will maintain a record of all authorized individuals that are not employees of the licensee who enter the Limited-Access Areas. The record will include the name of the individual, the company the individual works for, the reason the individual entered the Limited-Access Area, the date, and the times the individual entered and exited the Limited-Access Area.

11. All Limited-Access Area doors will remain closed and locked.

AUTHORITY
Section 26013, California Business and Professions Code
Reference: Sections 26070 and 26160, Business and Professions Code.
Bureau of Cannabis Control Proposed Text of Regulations
(Title 16, Division 42, Chapter 1, Article 5, §5042—California Code of Regulations)
(Title 16, Division 42, Chapter 1, Article 3, §5033—California Code of Regulations).

TRANSPORTING PRODUCT AND CASH

1. All cannabis product that is designated to enter the commercial supply chain will be transferred within the facility in accordance with the business's strict Track-and-Trace procedures.

2. All cash that is transferred within, into, or out of the facility will adhere to Divino Tessera's strict Security Procedures.

3. Cannabis products and/or cash that is transferred through, out of, or into the facility will be subject to the follow procedures:

    a) Products and/or cash will only be transferred by a Manager or a Quality Assurance Specialist

b) Products and/or cash transfers will immediately be recorded into company Sales Tracking software and the BioTrackTHC Track-and-Trace system
c) Managers and QA Specialists will be accompanied by a member of the Security staff any time cash is transferred within, into, or out of the facility.
d) Cash entering the facility will be immediately logged (Sales and Invoicing) and then immediately transferred to the Safe/Vault room

AUTHORITY
Section 26013, Business and Professions Code.
Reference: Sections 26012 and 26070, Business and Professions Code

DIGITAL SURVEILLANCE

1. 24-hour security surveillance cameras of at least HD-quality to monitor all entrances and exits to and from the building, all interior spaces within the facility which are open and accessible to the public, all interior spaces where cannabis, cash, or currency is being stored for any period of time on a regular basis, and all interior spaces where diversion of cannabis could reasonably occur.

2. Cameras will clearly show each point of sale location register with a time/date stamp.

3. Video recordings will be maintained for a minimum of one hundred twenty (120) days and will be made available to the City/State upon request. Video will be of sufficient quality for effective prosecution of any crime found to have occurred on the site of the commercial cannabis business.

4. The business will have a digital video surveillance system with a minimum camera resolution of 1280 x 1024 pixels.

5. The surveillance-system storage device will have transmission control protocol (TCP) capable of being accessed through the internet.

6. The video surveillance system is at all times able to effectively and clearly record images of the area under surveillance.

7. Each camera will be permanently mounted and in a fixed location. Each camera will be placed in a location that allows the camera to clearly record activity occurring within 20 feet of all points of entry and exit, and allows for the clear and certain identification of any person and activities in all areas required to be filmed.

8. Areas that are recorded on the video surveillance system include the following:

    a) Areas where cannabis goods are weighed, packed, stored, loaded, and unloaded for transportation, prepared, or moved within the licensed premises
    b) In the immediate interior and exterior areas of doors, windows, or other avenues of potential access
    c) Areas open to the public, including a full view of public right-of-way and any parking lot under the control of the Adult-Use Cannabis Business

d) Limited-access areas
e) Security rooms
f) Areas storing a surveillance-system storage device with at least one camera recording the access points to the secured surveillance recording area
g) Entrances and exits which are recorded from both indoor and outdoor vantage points

9. Cameras record continuously 24 hours per day and at a minimum of 15 frames per second (FPS).

10. The media storage device on which surveillance recordings are stored is secured in a manner to protect the recording from tampering or theft.

11. Surveillance recordings are kept for a minimum of 90 calendar days.

12. Surveillance recordings are available for inspection by the City and State, and will be kept in a manner that allows the City and State to view and obtain copies of the recordings immediately upon request. The licensee will also send or otherwise provide copies of the recordings to the City and State upon request within the time specified.

13. Recorded images clearly and accurately display the time and date. Time is measured in accordance with the standards issued by the United States National Institute of Standards and Technology standards.

14. The video surveillance system is equipped with a failure notification system that provides notification of any interruption or failure of the video surveillance system or video surveillance-system storage device.

AUTHORITY

Section 26013, Business and Professions Code.
Reference: Section 26070, Business and Professions Code.
Regulation 3.A.8(a)—Ordinance 185344 Rules and Regulations for Cannabis Procedures.
Bureau of Cannabis Control Proposed Text of Regulations
(Title 16, Division 42, Chapter 1, Article 5, §5044—California Code of Regulations).

ALARM SYSTEM

1. An alarm system managed by <Insert> will be monitored and operated 24 hours a day, 7 days a week.
2. Upon request, Divino Tessera will make available to the City and State, all information related to the alarm system, monitoring, and alarm activity.
3. A single alarm system covering the entire building is utilized for all operations within the building.
4. The security alarm system includes sensors to detect all points of entry and exit, from all limited-access and secured areas, all roof hatches, and all windows.

5. Divino Tessera will obtain a security alarm system permit that will be kept in good standing pursuant to LAMC Section 103.206.

AUTHORITY

Regulation No. 10.A.10, Ordinance 185344—Rules and Regulations for Cannabis Procedures.
Bureau of Cannabis Control Proposed Text of Regulations
(Title 16, Division 42, Chapter 1, Article 5, §5047—California Code of Regulations).

COMMERCIAL-GRADE LOCKS

1. The following areas are secured using commercial-grade, non-residential door locks, roof hatches, and window locks in a manner that prevents free and unauthorized access:
    a) All points of ingress and egress tos a premises.
    b) Limited-access areas
    c) Areas where cannabis goods, living cannabis plants, cannabis waste, and currency are stored and/or present at any given time
    d) Areas where surveillance equipment and records are stored

AUTHORITY

Section 26013, California Business and Professions Code.
Reference: Section 26070, Business and Professions Code.
Regulation No. 10.A.9—Ordinance 185344, Rules and Regulations for Cannabis Procedures
Bureau of Cannabis Control Proposed Text of Regulations
(Title 16, Division 42, Chapter 1, Article 5, §5046—California Code of Regulations).