Changing Address of Business

First Step: Occupational License (OL)

Log onto your online DMV OL Portal https://www.dmv.ca.gov/portal/mydmv

Go to My Licenses → License Overview → Modify → Select the type of change

You must complete the checklist. After submission the OL Department will schedule an inspection. Once the Occupational License is issued, please download, sign and send back so we can start Step 2.

Second Step: BPA Permit

Complete the forms to get a BPA Permit for each new location. You will need the following forms for ***each*** location.

- **BPA Modification Application** (Reg 4026)
- Security Questionnaire
- EXEC 201X
- EXEC 5555b
- Floor Plan
- Key Management Form
- Copy of the OL Permit
- Photos of the following items:
    - Front door and all entries for construction/ANSI Grade 1 locks
    - Picture of the front of the building with street and/or suite number
    - Security System – alarm and/or cameras
    - Workstation(s)
    - Storage – file cabinet or safe for all inventory and/or working documents.

Once you have completed these steps above, please send me all the paperwork, including the check for adding offices and a copy of the OL Permits. Send paperwork to:

ADR/SambaSafety
Attn: BPA Compliance
11040 White Rock Rd, Ste. 200
Rancho Cordova, CA 95670
bpacompliance@sambasafety.com
(800) 888-3317

STATE OF CALIFORNIA
DMV
DEPARTMENT OF MOTOR VEHICLES
A Public Service Agency

BUSINESS PARTNER AUTOMATION PROGRAM
APPLICATION FOR CHANGES

SITE ID

PLEASE TYPE OR PRINT CLEARLY

NAME *(IF CHANGING NAME OF COMPANY PRINT PRIOR NAME)*

Check appropriate box(es) for change(s) being made:

- ☐ Closing site
- ☐ Changing business, corporate name, Limited Liability Company (LLC) name, or DBA name
- ☐ Adding site
- ☐ Changing address of principal place of business or site
- ☐ Adding employee ☐ Deleting employee
- ☐ Changing controlling director(s) and/or officers
- ☐ Changing members of Limited Liability Company
- ☐ Change of Partner(s) or Stockholder(s)
- ☐ Change of floorplan and/or adding a terminal
- ☐ Changing processing address only

CHANGING COMPANY NAME — Meeting minutes for corporate name change *MUST BE ATTACHED*

PRINT NEW NAME

ADDING OR CHANGING ADDRESS

NEW ADDRESS *(NUMBER AND STREET)* | TELEPHONE NUMBER ( )

CITY | STATE | ZIP CODE

PRIOR ADDRESS IF CHANGING *(NUMBER AND STREET)* | TELEPHONE NUMBER ( )

CITY | STATE | ZIP CODE

ADDING OR DELETING EMPLOYEES (The Business Partner must notify the department of all employee changes) Each employee being added must submit a personal history questionnaire and have live scan fingerprinting done.

EMPLOYEE **ADDED** OR **DELETED** (*CHECK APPROPRIATE BOX*) ☐ **ADD** ☐ **DELETE** | DATE EMPLOYEE **ADDED** OR **DELETED**

TRUE FULL NAME *(LAST, FIRST, MIDDLE)* | BIRTH DATE | DL OR ID NUMBER | STATE ISSUED

RESIDENCE ADDRESS *(NUMBER/STREET)*

CITY | STATE | ZIP CODE

EMPLOYEE **ADDED** OR **DELETED** (*CHECK APPROPRIATE BOX*) ☐ **ADD** ☐ **DELETE** | DATE EMPLOYEE **ADDED** OR **DELETED**

TRUE FULL NAME *(LAST, FIRST, MIDDLE)* | BIRTH DATE | DL OR ID NUMBER | STATE ISSUED

RESIDENCE ADDRESS *(NUMBER/STREET)*

CITY | STATE | ZIP CODE

CERTIFICATION

I agree to notify the department in writing of any change in location, ownership, or legal structure of this business and to submit new Business Partner Automation Program application properly reflecting the changes together with the required fees. I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATE	PRINTED NAME	EMAIL ADDRESS
	SIGNATURE OF AUTHORIZED AGENT **X**	TITLE

ADDING OR DELETING DIRECTOR(S)/OFFICER(S)/PARTNER(S)/STOCKHOLDER(S)/MANAGEMENT/SUPERVISORS

If adding or deleting director(s)/officer(s)/partner(s)/stockholder(s)/management/supervisors, list all director(s), officer(s), partner(s), stockholder(s), management, and supervisors who, by reason of the facts and circumstances, could direct, control or manage the business partner office. If there are additional names, please attach a list.

Please note: Each individual listed below as being added must submit a Personal History Questionnaire and have Live Scan fingerprinting completed.

DATE ADDED	DATE DELETED	TRUE FULL NAME (Last, First, Middle)	TITLE

CERTIFICATION

I agree to notify the department in writing of any change in location, ownership, or legal structure of this business and to submit new application papers properly reflecting the changes together with the required fees. I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATE	SIGNATURE OF INDIVIDUAL OWNER, ANY PARTNER, AN OFFICER OF CORPORATION, OR MEMBER LLC	TITLE
	X	

ADDING OR DELETING MEMBER(S) OR MANAGER(S) LIMITED LIABILITY COMPANY

If adding or deleting member(s) or manager(s) of a limited liability company, list all controlling member(s) or manager(s) who, by reason of the facts and circumstances, could direct, control or manage the business partner office. If there are additional names, please attach a list.

Please note: Each individual listed below as being added must submit a Personal History Questionnaire and have Live Scan fingerprinting completed.

DATE ADDED	DATE DELETED	TRUE FULL NAME (Last, First, Middle)	TITLE

CERTIFICATION

I agree to notify the department in writing of any change in location, ownership, or legal structure of this business and to submit new application papers properly reflecting the changes together with the required fees. I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATE	SIGNATURE OF INDIVIDUAL OWNER, ANY PARTNER, AN OFFICER OF CORPORATION, OR MEMBER LLC	TITLE
	X	

IF CORPORATION, CORPORATE SEAL MUST BE PRESENT

STATE OF CALIFORNIA
DMV
DEPARTMENT OF MOTOR VEHICLES

A Public Service Agency

INFORMATION
SECURITY AND DISCLOSURE STATEMENT
FIRM

FIRM NAME

FIRM ADDRESS

TELEPHONE NUMBER

The California Department of Motor Vehicles (CADMV) collects confidential and personal information from the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various state and federal laws and regulations including the Information Practices Act, the Public Records Act, the California Vehicle Code, and the State Administrative Manual. The CADMV is committed to protect this information from unauthorized access, use, or disclosure. Policies pertaining to the DMV information are as follows:

I have read and I understand the following provisions of California Vehicle Code Section 1808.47:

> "Any person who has access to confidential or restricted information from the department shall establish procedures to protect the confidentiality of those records."

Pursuant to the above, I understand the following are my responsibilities:

1. To protect the confidentiality of any residence address information provided to me by and on behalf of CADMV.

2. As an authorized representative and/or corporate officer of the firm named above, I warrant that my firm and its employees will not disclose or alter any documents, diagrams, information, or information storage media made available to us by the CADMV. Any information copied (electronically, physically or otherwise) shall be for the sole purpose of adhering to the attached agreement. I warrant that only those employees who are required to use such materials will have access and authorization to them. Prior to receiving authorization as a CADMV information user, I will require each employee, whom I authorize to have access to CADMV data, to immediately and annually read and sign an "Information Security and Disclosure Statement Public/Private Partnerships (Employee)," EXEC 200X. One copy will be kept by the employee, the original kept by our management.

3. I warrant that my firm and its employees will access and use the information provided to me by the CADMV solely for the purpose specified in the attached Agreement. I warrant my firm and its employees will not access or use CADMV information for personal reasons. (An example of inappropriate access or misuse of CADMV information is memorizing or copying a residence address from a CADMV document or electronic record for any reason that is not related to job responsibilities.)

4. I warrant that my firm and its employees will not, in any way, distribute, sell, or alter the information provided by the CADMV.

5. I warrant my firm and its employees will not deliberately perform unauthorized additions, alterations, or deletions to existing data, or enter false or incomplete data on any CADMV document or computer data file.

6. Once the functions specified in the Agreement have been performed, I warrant that my firm and its employees as directed by the CADMV will physically destroy or electronically erase (degauss) the medium containing any CADMV information.

7. I warrant my firm and its employees shall provide secure storage and accountability for all CADMV information and copies of information.

8. I warrant that my firm and its employees shall take precautions to create a secure password. A secure password is one that cannot be associated with the firm, its employees or their interests. Passwords are not to be revealed to any person or firm, nor recorded on any document. If there is reason to believe anyone has determined the nature of a password, that password shall immediately be changed.

9. I warrant that my firm and its employees shall take reasonable precautions to protect terminals, equipment, and systems from unauthorized access. Reasonable precautions include, but are not limited to: not leaving unattended terminals logged on to a system accessing CADMV data; storing user instructions or manuals in a secure place; moving documents to be destroyed to a secure and confidential area pending destruction; not removing documents from the firm's premises; reporting any suspicious circumstances or unauthorized individuals observed in the work area.

10. I understand and acknowledge that it is a public offense to knowingly and without permission alter, damage, delete, destroy, copy, or otherwise use any CADMV data. Such action may result in civil or criminal prosecution, and is punishable by fine and imprisonment.

11. Federal Law states:

    "Any person who knowingly obtains, discloses, or uses personal information from a motor vehicle record for a purpose not permitted under the Driver's Privacy Protection Act (Title 18 of the United States Code, Section 2721 - 2725), shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court. The court may award:

    - *actual damages, but not less than liquidated damages in the amount of $2,500;*
    - *punitive damages upon proof of willful or reckless disregard of the law;*
    - *reasonable attorney's fees and other litigation costs reasonably incurred; and*
    - *such other preliminary and equitable relief as the court determines to be appropriate."*

I certify under penalty of perjury, under Federal rules and regulations and the laws of the State of California, that the above statements are true and correct. I have read and understand the security policies stated above and have received a copy of them.

Executed at: _____
CITY COUNTY STATE

_____ _____
SIGNATURE OF AUTHORIZED FIRM REPRESENTATIVE **DATE**

_____
PRINTED NAME AND TITLE OF SIGNATORY

_____
PRINTED NAME OF FIRM:

_____

STATE OF CALIFORNIA
DMV
DEPARTMENT OF MOTOR VEHICLES
A Public Service Agency

BUSINESS PARTNER AUTOMATION PROGRAM
INFORMATION SECURITY PRE-IMPLEMENTATION CHECKLIST

SECOND-LINE BUSINESS PARTNER

BUSINESS PARTNER NAME				TELEPHONE NUMBER
				( )
BUSINESS ADDRESS	CITY	STATE	ZIP CODE	SERVICE PROVIDER
				ADR

USE THE NUMBER LISTED ON THIS CHECKLIST TO IDENTIFY THE NARRATIVE, DIAGRAM, FLOOR PLAN, OR SUBMITTED MATERIAL WHEN PUTTING YOUR PACKAGE TOGETHER. ***Place this form on top of the completed package.***

To assure a secure environment is maintained, DMV requires administrative measures and minimum standards are met by the First-Line Business Partner Service Provider *(FLBPSP)* and their Second-Line Business Partner (*SLBP)*. To ensure that DMV measures and standards are met prior to implementation the partners must provide the following information or documents:

GENERAL SECURITY INFORMATION

☑ 1. Provide one (1) copy each of the FLBPSP security policies and or the Information Security Program policies; user guide or processing manual; and guidelines or Training Manual(s) for physical and electronic access for SLBP staff authorized to work with DMV resources and assets.

☑ 2. Provide a description of the Business Partners' process(es) for identifying possible security incidents. Identify what procedures or process(es) are utilized to prevent further security violation(s) after they are found, and how a security violation is documented and reported to DMV.

RESOURCE AND ASSET PHYSICAL SECURITY

☑ 3. Provide a floor plan and a detailed narrative describing workstation and facility security. The documentation must include overall facility security and intrusion prevention, entry control measures, as well as detail regarding the area(s) where DMV resources and assets are used, or stored (permanent and working storage), and where electronic data manager workstations and printers are located. Include details regarding security control measures *(i.e., the location and descriptions of any safe(s) or file cabinet(s) used for DMV controlled and accountable items security; identify areas that are public and employee and authorized employees only; details regarding facility security measures (i.e., alarm or surveillance systems); and identify the locations of internal and external doors, window, and other openings and how they are secured)*.

ACCESS SECURITY

☑ 4. Provide a narrative that details how users are IDENTIFIED, AUTHENTICATED, and AUTHORIZED access to DMV BPA processes, resources, and assets.

RETENTION AND DESTRUCTION SECURITY

☑ 5. Provide a narrative that details how DMV information resources are secured and kept private while retained or captured via any method and or medium (electronic or physical), fixed or portable.

☑ 6. Provide a narrative that details how DMV information resources and assets are rendered un-readable, un-useable, and un-recoverable after legitimate business use has ended or destruction is required.

DECLARATION STATEMENT

As th Authoriz or D signat r pr s ntativ of: _____
BUSINESS NAME

I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

PRINTED NAME OF AUTHORIZED REPRESENTATIVE

SIGNATURE OF AUTHORIZED REPRESENTATIVE	DATE
✍	

Security Questionnaire
ADR / CABPA Program

To assure a secure environment is maintained, the California Department of Motor Vehicles (CADMV) requires administrative measures and minimum standards are met by ADR, a First Line Business Partner Service Provider (FLBPSP), and our customers who are Second Line Business Partners (SLBP). To ensure that CADMV measure and standards are met prior to service implementation, ADR must provide information and documents in response to a California DMV Business Partner Automation Program, Business Partner Pre-Implementation Checklist (*Ref. DMV INV 5555B*) for review and approval by the CADMV. By providing the following information you are assisting in preparing this response package.

_____ _____

(Business Name) ***(Business Address)***

_____ _____ _____

(Name of the Authorized or Designated Representative) ***(Phone Number)*** ***(E-Mail address, if available)***

General Security Information

- The client shall implement the physical security measures and methods stated in this Agreement to prevent and discourage inadvertent or deliberate alteration, disclosure, destruction, loss, misuse, or theft of the DMV records, and proprietary assets under their control.

- The client shall be responsible for making sure it prevents access to DMV records (retained in any portable medium or method), and proprietary assets by the general public and other un-authorized individuals.

- The client shall prevent the unauthorized viewing of DMV proprietary assets displayed by any medium or method. The client shall require workstations and printers utilized to access the DMV vehicle registration and titling and inventory databases, display or print DMV records, be located within the facility in such a manner that displayed or printed records are not visible or accessible to unauthorized employees or the general public.

- The client shall provide a secure business site or facility. Business site or facility entries shall be equipped with doors or closures that are of solid construction and are equipped with positive locking devices such as dead bolt type locks. The client shall secure all external windows, skylights, and vents, to the business site or facility in such a manner as to prevent entry, and preclude viewing into any areas of the business site or facility where DMV proprietary assets are stored.

- The client shall not leave DMV proprietary assets retained in any portable medium or method under their control un-attended when not secured in a device or location specified by this Agreement.

- The client shall secure DMV proprietary assets retained in any portable medium or method, under their control in a safe or cabinet of metal construction that is built into, or is permanently attached to, the business site or facility, unless the safe or cabinet is of sufficient size (at least four (4) feet in height or width) or weight (at least on hundred fifty (150) pounds) to substantially preclude it from being readily removed from the business site or facility, during non-business hours. The safe or cabinet shall be equipped with a positive locking device(s) and the Service Provider shall restrict and control knowledge of, and use of, the method for un-locking to individuals that have completed and signed an *Information Security and Disclosure Statement, Public and Private Partnerships Employee* form, which is incorporated by reference and made part of this Agreement submitted during the application process for participation in the BPA program.

- The client shall secure DMV proprietary assets retained in any portable medium or method under their control during business hours in a device that is not readily portable (e.g., in a large metal cabinet, desk, or workstation drawer) and is equipped with a positive locking device. The client shall implement physical barriers that prevent the general public and other unauthorized individuals from having access to the secure storage device and restrict and control knowledge of, and use of, the method for unlocking the device to individuals that have completed and signed an *Information Security and Disclosure Statement, Public and Private Partnerships Employee* form.

- The client shall place network and system devices used in the BPA program and DMV interface in secure areas. The client shall control access to these devices and shall prohibit access to and view of (if appropriate), these devices to individuals that

have completed and signed an *Information Security and Disclosure Statement, Public and Private Partnerships Employee* form submitted during the application process for participation in the BPA program.

Resource and Asset Physical Security

Business Facility Diagram

Please prepare a simple diagram of your business facility that shows the location of all external and internal doors, windows, or other openings; and the placement of rooms/offices, counters, partitions, and desks. Additionally, using the legend below, mark the locations of the following items on your diagram:

C → Place a "**W**" where each workstation (computer) utilized for CADMV access is location and an arrow (→) coming from the "W" to indicate the direction in which the workstation screen is facing.

P Place a "**P**" where each printer utilized is located.

I Place an "**I**" where CADMV inventory (License plates/stickers/DMV paper) is stored.

Business Facility Questions (Please answer in the space provided)

Please answer the following questions about your business facility:

- **Will DMV inventory be stored at this facility?** Yes _____
- **What security and/or intrusion prevention or entry control measures are in place to protect your business facility's external windows, openings, and doors during non-business hours?**

  a. Does your business facility have an alarm or surveillance system? _____

  b. Do you employ a security guard/patrol service during non-business hours? _____

  c. If your business facility does not have an alarm or surveillance system; or a security guard/patrol service, what other security and/or intrusion prevention methods or devices have you implemented to protect your business facility's external windows, openings, and doors during non-business hours?

  _____

- **What are the business facility entry door(s) constructed of (i.e., solid wood, glass, glass/metal frame, metal, etc.)?**

  _____

  a. What type of lock(s) or locking device(s) are the door(s) equipped with (i.e., deadbolt lock, locking braces, or pins, etc.)?

  _____

- **On the diagram where you indicated that the workstation(s) (W) and printer(s) (P) are placed please respond to the following questions** *(You may answer questions in the space provided and transfer them later to the diagram):*

  a. Are workstation(s) and printer(s) placement in a private area with restricted access to unauthorized viewing? _____

  a. If workstation(s) screens or printers are visible from any external or internal windows or open areas, how is viewing by the public or unauthorized employees (unauthorized personnel) precluded (i.e., by the use of window blinds, curtains, or tinting; or by the placement of a partition or the use a screen hood, etc.)?

  _____

  b. How is access by unauthorized personnel controlled to the office, room, or area where computer(s) and printer(s) are located (i.e., locked doors; controlled entry doors, key or pass card controlled; by a receptionist with a separate waiting area away from the workstation(s) and printer(s) placement, and only one client at a time allowed at work area etc.)?

  _____

- **On the diagram where you indicated that CADMV inventory (I) (License plates/stickers/DMV paper) is stored, please respond to the following questions:**

  a. What devices are utilized to securely store CADMV inventory:

     - For permanent storage (e.g., Main storage/Non-business hour storage) (i.e., a metal safe or cabinet; a metal cage etc.)

_____

     - For "working" inventory storage (e.g., Workstations/Counter storage only during business hours) (i.e., lockable desk drawer, lockable file cabinet, etc.)?

_____

  b. Is the device used for permanent storage 150 pounds or more unloaded and at least four feet high or four feet wide?

     Yes _____ No _____

  c. Is the permanent storage device fastened to the facility and how is this accomplished? (Note: Fastening is not required if the device is over 150 pounds unloaded and at least four feet high or four feet wide.)

_____

  d. What type of positive locking method(s) are the storage devices equipped with (i.e., built in combinations or deadbolt key lock; electronic lock, combination or keypad lock, etc.)?

     Permanent Storage _____ Working Storage _____

  e. How is access by the public and unauthorized employees controlled to the office, room, or area where the devices(s) utilized for CADMV inventory storage, permanent and working, are located (i.e., locked door(s), same controls as for the area where the workstation(s) (computer(s)) and printer(s) are located, etc.)?

_____

Access Security

- All client employees with direct or incidental access to CADMV computers, printers, information, and inventory items must complete and sign an *Information Security and Disclosure Statement, Public and Private Partnerships Employee* form (EXEC200X) at the time of hire or the granting of access, and annually thereafter for a long as access is authorized. The forms must be maintained for three (3) years following each removal or expiration of an individual's access authorization, and be available, upon written request, to CADMV.

- All clients and employees with CABPA access will provide a valid California driver's license or ID number, Social Security number, and residence address.

- All clients and employees with CABPA access must understand the following:
  a. Proper procedures for use of the program.
  b. Constraints upon use and disclosure of information made available through the program.
  c. Sanctions for misuse of the program or information.

- Workstations shall not be left unattended while accessing DMV vehicle registration and titling or inventory database. Workstations shall be configured to either programmatically end access or invoke a display obfuscation screen after a maximum of ten (10) continuous minutes of inactivity. Once access has ended or the display screen has been obfuscated, the user shall be required to re-authenticate to the authentication credentialing system prior to re-establishing access or un-obscuring the display.

- All clients or employees with intent to access the CABPA program will establish a unique individual password. When establishing or changing password(s), all individuals accessing the CABPA program will adhere to the following standards:

a. Passwords are a minimum of six (6) and a maximum of eight (8) characters, comprised of both numbers and letters.
b. Identical passwords will not be used more than once by the same individual within a two (2) year period.
c. Passwords will not be shared, displayed, written down, or otherwise kept in a locations here they can be seen or obtained by anyone other than the person to whom they belong.
d. Passwords will be changed once every sixty (60) days. The ADR system will automatically prompt the user to change passwords at necessary intervals.
e. Second Line Business Partner clients and employees may elect to change passwords prior to expiration if they feel the current password is compromised.

Retention and Destruction Security

- The SLBP is responsible for the security of all system workstations and content. Security measures used by the SLBP must follow, but are not limited to the following:

  a. All locks to which an employee has keys should be changed when an employee discontinues employment.
  b. CADMV Inventory not in current business use should be kept appropriately locked.
  c. Authorized employees no longer endorsed for CABPA access should conduct inventory audits with their direct supervisor upon terminating access to the CABPA program.

- All inventory received for the CABPA program must be verified against the shipping receipt upon delivery. All inventory discrepancies (i.e., missing plates and stickers), must be reported appropriately upon discovery.

- The client shall not transfer, retain, or store any DMV proprietary assets or records on any portable electronic medium such as diskettes, CD-ROMs, removable memory chips, or magnetic tapes.

- The client shall place network and system devices used in the CABPA program and CADMV interface in secure areas. The client shall control access to these devices and shall prohibit access to, and viewing of (if appropriate), these devices to individuals that have not completed and signed an Information Security and Disclosure Statement, Public and Private Partnerships Employee form submitted during the application process for participation in the BPA program.

- Workstations displaying DMV records or the DMV vehicle registration and titling or inventory database information shall display an electronic "admonishment warning banner" to the user at the time of access initiation. The banner shall contain the following language: "WARNING: Unauthorized access or misuse of data may result in disciplinary action or civil penalties and/or criminal prosecution."

- No "working inventories of CADMV items (License plates/stickers/DMV paper) are to be maintained outside of the permanent secure storage device during non-business hours. All CADMV inventories are to be kept in the device(s) previously designated and described.

- No DMV information shall be electronically stored away from the ADR computer system. No customer private or confidential information such as residence address shall be kept on the computer hard drive, or kept via any portable recording method.

- Obsolete and damaged CADMV inventory must be recorded with ADR/CADMV before it is destroyed. The method of destruction must assure that the CADMV inventory item is rendered unusable, unreadable, and unrecoverable.

- All DMV paperwork shall be destroyed after legitimate business use has ended. The method of destruction (i.e., shredding) shall assure that the information contained on the paperwork is rendered unusable, unreadable, and unrecoverable.

_____ _____

Business Name Signature

_____

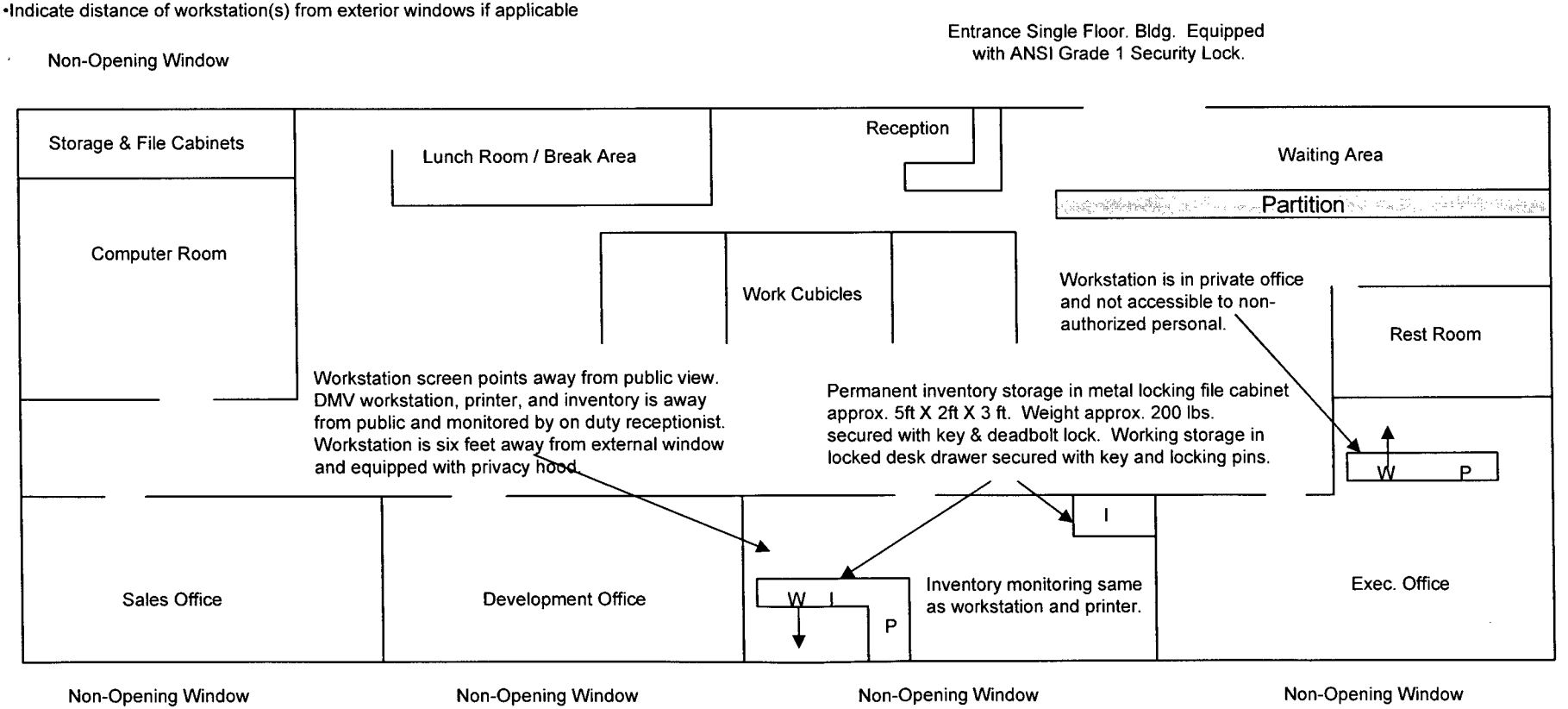
Date

FLOOR PLAN SAMPLE & INSTRUCTIONS

FROM BUSINEES FACILITY QUESTIONS OF THE SECURITY QUESTIONAIRE INCLUDE THE FOLLOWING INFORMATION ON THE BUSINESS DIAGRAM.

A.D.R Registration Services
1 City Blvd W. Suite 1440, Orange Ca., 92868

- •Name and address at top of floor plan.
- •Location of all doors, windows and stairs if more than one floor.
- •Directional sign indicating north, south, east, and west.
- •Position of offices, cubicles, and walls and partitions. Label all partitions.
- •Position of workstation(s) and printer(s) for DMV use. (Workstation designated with "W" and printer with "P")
- •Indicate with an ⟶ coming from the "W" which way workstation(s) screens are facing.
- •If workstation screens are visible to unauthorized personnel, indicate how viewing is prevented.
- •Indicate how access to DMV workstations and printers by unauthorized persons is controlled.
- •Location of inventory repositories designated with "I" for both permanent and working storage.
- •Indicate what devices are used for permanent and working storage of DMV Inventory.
- •Indicate estimated measurements and weight of device used for permanent storage.
- •If storage device is under "minimum stand alone" requirements, indicate how device is made secure.
- •Note what type of locking methods inventory storage devices are equipped with.
- •Indicate how unauthorized access is controlled to inventory storage area(s).
- •Indicate if exterior doors are equipped with ANSI Grade 1 Security Locks.
- •Indicate distance of workstation(s) from exterior windows if applicable



Attachment 1

PHYSICAL KEY MANAGEMENT CONTROLS

Business Name	
Facility Address	
Prepared by	

	Are The Following Key Management Controls In Place?	In Place	Not In Place	Target Date
1	A **policy** for the issuance and collection of all business facility keys.	☐	☐	
2	A **method/program** for tracking the issuance and collection of all keys.	☐	☐	
	(a) The above key tracking method/program is: ☐ A manual method ☐ A dedicated computer software application	☐	☐	
3	We have a designated ☐ Key Control Authority and/or ☐ Key Control Manager to *implement*, *execute*, and *enforce* key control policies and procedures	☐	☐	
4	Our designated Key Control Official also executes the following functions: (a) Develops and keeps current a list of personnel that have authorized access to the area(s) and components where CADMV proprietary information resides.	☐	☐	
	(b) Reviews and approves the access list and authorization credentials.	☐	☐	
	(c) Promptly deletes access of personnel no longer requiring access to the area(s) and components where CADMV proprietary information resides.	☐	☐	
5	Physical access devices; such as keys, locks, combinations, card readers, etc., to control entry points to the location(s) where CADMV proprietary information resides.	☐	☐	
6	Keys (and key blanks, if applicable) are locked in a cabinet/container in a secured area.	☐	☐	
7	Inventory keys, combinations, and other access devices are secured regularly.	☐	☐	
8	Keys are issued to individuals who have a legitimate and official requirement for the key.	☐	☐	
9	Combinations and keys are changed periodically. ☐ Annually ☐ Other:	☐	☐	
10	Combinations and keys are changed when keys are lost, combinations are compromised, or individuals are transferred or terminated.	☐	☐	

Above recommendations are based on NIST Special Publication 800-52 (Appendix F-PE; pages F-50, F-51), and *Guide to Developing and Managing Key Control Policies and Procedures, by ASSA ABLOY, as found at http://www.medeco.com/techsvc/pdf/LT-922093RevA.pdf*