STATE OF CALIFORNIA
DEPARTMENT OF MOTOR VEHICLES
A Public Service Agency

INTERSTATE CARRIER PROGRAM (ICP) SECURITY AGREEMENT

Print Clear Form

STATE OF CALIFORNIA
DEPARTMENT OF MOTOR VEHICLES
A Public Service Agency

CALIFORNIA DEPARTMENT OF MOTOR VEHICLES
ICP SECURITY AGREEMENT

SECTION 1 — INTRODUCTION

The California Department of Motor Vehicles (CADMV) is the principle provider of International Registration Plan (IRP) services. As evidence of its commitment to expand delivery options for its products and services, the CADMV developed the Interstate Carrier Program (ICP).

Veh. Code §1685.1 authorizes qualified ICP partners to access CADMV's IRP System at their approved location to process interstate registration for apportioned vehicles. This access provides the ICP partner with the capability to initiate registration transactions, payment for fees through electronic fund transfer, and complete transactions in order to issue IRP registration indicia on-site.

SECTION 2 — ICP PARTNER PRIMARY LOCATION

BUSINESS NAME		TOTAL NUMBER OF AUTHORIZED ICP WORKSTATIONS

BUSINESS ADDRESS	CITY	STATE	ZIP CODE

SECTION 3 — ADDITIONAL BRANCH LOCATION(S)

BUSINESS NAME		TOTAL NUMBER OF AUTHORIZED ICP WORKSTATIONS

BUSINESS ADDRESS	CITY	STATE	ZIP CODE

BUSINESS NAME		TOTAL NUMBER OF AUTHORIZED ICP WORKSTATIONS

BUSINESS ADDRESS	CITY	STATE	ZIP CODE

SECTION 4 — AUTHORIZED ICP PARTNER REPRESENTATIVE

NAME	POSITION/TITLE

EMAIL ADDRESS	TELEPHONE NUMBER
	( )

Print Clear Form

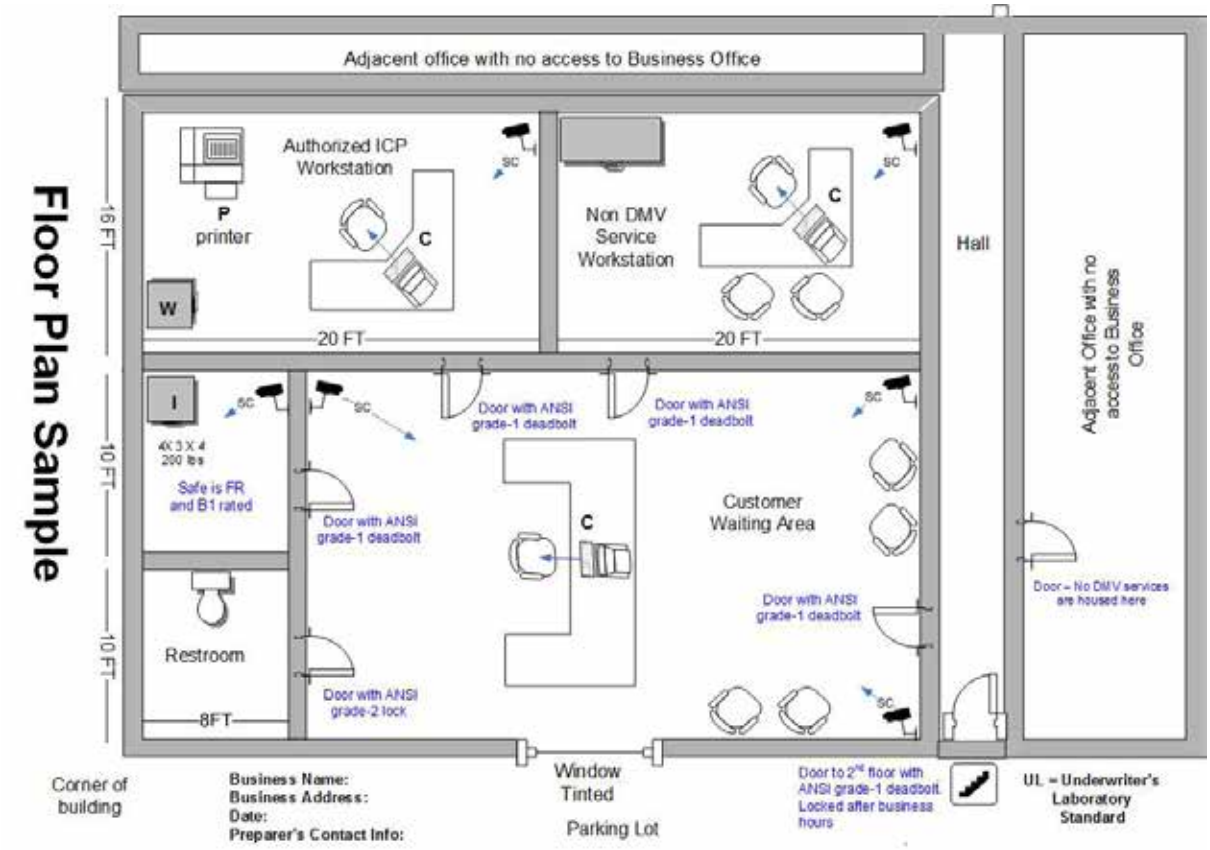
SECTION 5 — FLOOR PLAN DIAGRAM (*See Sample Below)*

ICP partners must provide computer-generated floor plans for all locations that process ICP transactions with the following requirements:

1. Identify all interior and exterior barriers and entrances including doors (type of lock installed i.e., ANSI Grade #1), walls (floor to ceiling), partitions, windows, skylights, etc.
2. Identify all interior placement of counters, office furniture, workstations, printers, safes, and cabinets.
3. Identify all areas/rooms including Authorized ICP Workstations, inventory rooms, customer waiting areas, break rooms, offices, and restrooms.
4. The Authorized ICP Workstation and Inventory Room must be enclosed with floor-to-ceiling constructed walls and only accessible through a door equipped with ANSI Grade #1 locks. Both rooms must be monitored by Security Cameras.
5. Include the dimensions (in feet) of the office as well as the individual rooms.
6. Label what is located on the exterior of all sides of the office (Example: parking lot, alley, adjacent business with no access to business office, etc.).
7. All floor plans must label the business name, business address, contact information of the person who prepared the floor plan, and the date of when the floor plan was prepared.

Use these symbols to identify the location of the following items on your floor plan diagram.

C →	Indicates computer locations and the direction the PC monitors are facing.
P	Indicates printer locations.
I	Indicates the permanent CADMV inventory storage location of metal safe or metal cabinet.
W	Indicates location of inventory storage during work hours (desks, cabinet, etc., if applicable).
SC →	Indicates location of security camera and the direction the camera is facing.



Print Clear Form

SECTION 6 — ICP SECURITY REQUIREMENTS

In order to participate in the ICP, all ICP partners must comply with the security requirements identified within the ICP Security Agreement (REG 216 I). Inability to meet a security requirement may result in denial of request to the ICP or discontinued enrollment. Additional information, beyond this document, may be required to determine if the ICP partner has appropriately implemented specific aspects of a security requirement.

	Physical Security	Agreed
1	ICP partner assumes the responsibility of preventing unauthorized access and viewing of CADMV proprietary records and assets.	☐
2	Exterior facility entry doors or closures are of solid construction (e.g., tempered glass and metal frame, solid wood, or steel, etc.)	☐
3	Exterior facility doors are equipped with positive locking devices such as mortise and latch; lever and/or dead bolt locks that meet American National Standards Institution/Builders Hardware Manufacturers Association (ANSI/BHMA Grade #1) standards.	☐
4	Exterior facility windows, skylights, and vents are secured in such a manner as to prevent unauthorized entry or viewing into areas where CADMV proprietary assets are stored.	☐
5	Blinds, tinting, screens or other devices are in place on exterior and interior windows to prevent unauthorized viewing of monitors and printed documents.	☐
6	Workstations shall not be left unattended while accessing the CADMV's IRP system.	☐
7	The Authorized ICP Workstation and Inventory Room must be enclosed with floor-to-ceiling constructed walls and only accessible through a door equipped with ANSI Grade #1 locks.	☐
8	Workstations and printers used to process or print CADMV records must be secured to the business site by means of a security cabling system, or physically affixing the workstation or printer to an enclosure or fixture/furniture located within the facility.	☐
9	ICP partner designates a printer only for registration transactions that are utilized only by authorized users.	☐
10	Workstation components (PC, monitors, and printers) are placed in secure areas to limit access and viewing of workstation components only to authorized ICP users approved by CADMV.	☐
11	The business facility is equipped with a functioning camera and alarm for site surveillance.	☐
12	Alarm and video surveillance systems monitor all points of entry to the facility, authorized workstations and location of CADMV Inventory.	☐
13	Alarm and video surveillance systems are monitored in real time to identify and respond to security incidents.	☐
14	Alarm system is to be activated during non-business hours.	☐
15	Site surveillance videos are stored for at least six (6) months before video is overwritten.	☐
16	CADMV proprietary assets are not left unattended, when outside of their secure device or location.	☐
17	During non-business hours, CADMV proprietary assets are secured in a metal safe or metal cabinet meeting or exceeding the following specifications: • The metal safe or metal cabinet is at least 4 feet high or 4 feet wide; and weighs at least 150 pounds when *empty*. • If the safe or cabinet is not of sufficient size or weight, it is permanently attached (bolted) to a facility wall or floor. • The safe or cabinet is equipped with a locking device such as a combination pad, a padlock, or a cabinet lock. • The knowledge and method for unlocking the safe or cabinet is restricted to authorized ICP users.	☐
18	During business hours CADMV proprietary assets are secured in a metal cabinet, a desk or workstation drawer equipped with a locking device.	☐
19	Physical access to network distribution and transmission lines within your facility is restricted to authorized personnel.	☐

Print Clear Form

	Physical Security (*Continued*)	Agreed
20	Physical access to output devices (e.g., monitors, printers, copiers) is restricted to prevent unauthorized individuals from obtaining the output.	☐
21	Information system components (e.g., monitors, servers) are physically positioned within the facility to minimize unauthorized viewing and access.	☐
	Computer System Security	**Agreed**
22	ICP partner's information system is configured to prohibit wireless access to CADMV systems.	☐
23	ICP partner installs all updates and patches all system software immediately as updates and patches become available from the software provider.	☐
24	Malicious code protection (anti-virus) mechanisms are implemented to detect and eradicate malicious code in critical entry and exit points, workstations, and servers of your organization's information system.	☐
25	Malicious code protection mechanisms are updated whenever new releases are available and include the latest malicious code definitions in accordance with organizational configuration management policy and procedures.	☐
26	Information system vulnerabilities are remediated immediately when discovered by malicious code protection or anti-virus mechanisms.	☐
	Access Control	**Agreed**
27	User ID requirements must include the following: • Each ICP user must have a unique user ID issued by CADMV. • ICP partner must notify CADMV when an ICP user is no longer employed by the ICP in order to deactivate their access account.	☐
28	Employees with direct or incidental access to CADMV workstation and proprietary assets must complete and sign the EXEC 200X statement at the time of hire or granting of access, and annually thereafter. See glossary for definition of EXEC 200X.	☐
29	The EXEC 200X is available to CADMV for 3 years after removal or expiration of an individual's access authorization, upon written request.	☐
30	Default passwords must be changed on first user logon.	☐

31	Passwords must contain the following requirements:
	• Be 8 or more characters in length.
	• Contain characters from each of the following 4 categories:
	  • English uppercase characters (A-Z).
	  • English lowercase characters (a-z).
	  • Base 10 digits (0-9).
	  • Special character (i.e. !@#$%^&* etc.).
	Passwords must be changed every 45 days.
		☐

32	ICP users must take specific measures to safeguard passwords such as: • Do not share your password. • Passwords shall not be written down or displayed in any plain text readable format. • Do not use names, surnames, pet names of family members, friends or pets, birthdays, anniversaries, or common phrases.	☐
33	The ICP user must change passwords if it is believed that a password has been compromised.	☐
34	Authorized ICP users are authenticated to the local network by means of username and password prior to logging in to the IRP System.	☐
35	Procedures are in place to disable CADMV access upon termination of an individual's employment.	☐
36	Upon termination of employment, all CADMV related property is retrieved from terminated personnel.	☐
37	Electronic and physical access authorizations to CADMV information are reviewed and terminated when personnel are reassigned or transferred to other positions within the organization.	☐

Print Clear Form

	Audit and Accountability	Agreed
38	ICP partner must maintain a Daily Transaction Summary Sheet (DTS). Content must include the following: • Transaction date. • Office number ID. • ICP user ID. • Transaction type. • Account number.	☐
39	DTS are retained for 4 years from date of generation.	☐
40	DTS are protected from unauthorized access, modification, and deletion.	☐
41	ICP partner reviews DTS content for indications for inappropriate or unusual activity at least monthly.	☐
42	ICP partner must maintain a documented list of all authorized ICP users that access CADMV information and be available to CADMV when requested. Authorized ICP user documentation must include: • Name. • Address. • DL or ID number and state. • Date of birth. • ICP user ID. • Period of time access permitted. • Workstations on which access was permitted. • Locations at which access was permitted.	☐
43	ICP partner must maintain a documented list of all workstations that access CADMV information and be available to CADMV when requested. Workstation documentation must include: • Make, model and serial number of the device. • Physical location. • Period of time access permitted. • ICP user ID of individual(s) having access to workstation. • Documentation must be maintained from 4 years following the last time the device is capable of access.	☐
44	ICP partner must provide the Global Network Address Translation (NAT) Internet Protocol (IP) address to CADMV by email response when requested by the department.	☐
	Proprietary Assets and Media Protection	**Agreed**
45	CADMV records are NOT retained or stored on portable media such as, but not limited to: CDs, DVDs, removable chips, USB devices, or magnetic tapes.	☐
46	CADMV proprietary assets and records (hard/electronic copies) are appropriately disposed of and destroyed.	☐
47	Disposed CADMV assets and records are rendered completely unreadable, unrecoverable, and unusable.	☐
48	ICP partner restricts access to CADMV proprietary assets only to authorized individuals.	☐
49	Obsolete and damaged inventory is recorded with CADMV before it is appropriately destroyed.	☐
50	All printers used to print CADMV documentation must be a standalone printer with limited functionality to prevent unauthorized wireless access or unauthorized information disclosure.	☐
51	All printers used to print CADMV documentation that contain any storage memory or hard drive must have a security kit installed to wipe any print data stored on those storage devices.	☐
52	CADMV information is not electronically combined, or linked with any third party database for resale or for any purpose not previously approved by CADMV.	☐

Print Clear Form

	Proprietary Assets and Media Protection (*Continued*)	**Agreed**
53	CADMV information is not stored beyond its intended business purpose, unless mandated by Federal or State record retention requirements.	☐
54	CADMV information media is protected until the media is destroyed or sanitized.	☐
55	All equipment used to process, transmit, or store CADMV information is sanitized.	☐
56	All paper documents containing CADMV data are appropriately destroyed after the legitimate business use has ended.	☐
	Security Incident Response & Reporting	**Agreed**
57	ICP partner ensures security incident reporting and privacy notification are consistent with the requirements of the California Information Practices Act of 1977 specifically Civil Code 1798.29.	☐
58	ICP partner must notify CADMV ICP Program Administrator by: • Email at **rodicpadministrators@dmv.ca.gov**. • Within 24 hours for any intrusion, theft, unauthorized disclosure, or unauthorized access of CADMV proprietary records or assets.	☐
59	ICP partner implements security incident handling capability and procedures for the following: • Detection. • Recording. • Analysis. • Containment. • Eradication/Remediation. • Recovery.	☐
60	ICP partner identifies, defines and documents appropriate actions and staff response to each type of security incident (e.g., security policy, procedures, malware, Distributed Denial of Service (DDOS) disclosure etc.)	☐
61	ICP partner provides annual security incident response procedures training to all new and current authorized ICP users (including managers, senior executives, and contractors) or when system changes are made. ICP partner must provide evidence of training to the department upon request.	☐
	Physical Key Management Controls	**Agreed**
62	A policy is in place for the issuance and collection of all business facility keys.	☐
63	A procedure is in place for tracking the issuance and collection of all keys.	☐
64	ICP partner has a designated Key Control Authority to implement, execute, and enforce key control policies and procedures.	☐
65	Key Control Authority must execute the following functions: • Develops and keeps current a list of personnel that have authorized access to the area(s) and components where CADMV proprietary information resides. • Reviews and approves the access list and authorization credentials. • Promptly deletes access of personnel no longer requiring access to the area(s) and components where CADMV proprietary information resides.	☐
66	ICP partner stores keys (and key blanks, if applicable) in a locked cabinet/container in a secured area.	☐
67	ICP partner inventories keys, combinations, and other access devices annually.	☐
68	ICP partner issues keys only to authorized individuals.	☐
69	ICP partner changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.	☐

Print Clear Form

SECTION 7 — CERTIFICATION

I have read and understand all of the requirements identified within this agreement and agree to comply with all requirements. I understand answers provided in this document are subject to an audit, inspection, or investigation. Any discrepancies found during the course of the review may be grounds for suspension or termination from the ICP. Any errors discovered in the above responses must immediately be brought to the attention of the ICP Administrators. Security controls identified in this document are subject to change to address newly discovered vulnerabilities or compliance with new or updated Federal and State requirements.

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

PRINTED NAME	TITLE

AUTHORIZED ICP PARTNER REPRESENTATIVE SIGNATURE	DATE
X	

Print Clear Form

GLOSSARY

ANSI – American National Standards Institute – oversees the creation, promulgations and use of thousands of norms and guidelines for the US marketplace. Directly engaged in accrediting programs that assess conformance to standards.

BHMA – Builders Hardware Manufacturers Association - A trade association for North American manufacturers of commercial builder's hardware. BHMA currently authors 33 ANSI/BHMA standards in the builder's hardware category.

CADMV – California Department of Motor Vehicles

EXEC 200X – Information Security and Disclosure Statement, Public/Private Partnerships Employee

Propriety Assets – are defined as inventory, all records, files, computer programs, data used to operate, including mailing lists, access control tables, printouts, lists, manuals, and publications, including but not limited to "Copyrighted or Trademarked" materials on which CADMV controls usage by others for specified purposes.

Security Incident – means the unauthorized taking, use, release, modification, damage, destruction, disclosure, loss, or access to information assets (see SAM §4845), whether by a CADMV officer or employee or some other person, including but not limited to:

i) taking, use, disclosure, modification, damage, or deletion of information held by or owned by CADMV.

ii) taking, use, release, modification, damage or destruction of equipment or software held by or owned by CADMV.

iii) Occurrence of a computer virus on or in a CADMV information asset.

iv) The presence of unauthorized software on a CADMV information asset.

v) The otherwise authorized use of an information asset in the commission of a crime.

Print Clear Form