COUNTY OF EL DORADO, CALIFORNIA
BOARD OF SUPERVISORS POLICY

Subject:	Policy Number:	Page Number:
DMV DATA ACCESS POLICY	A-12	1 of 3
	Originally Adopted: 11/14/2023	Last Revised Date: 11/14/2023

I. Purpose

The purpose of this policy is to:

A. Define the requirements for employees and departments with State of California Department of Motor Vehicle (DMV) access
B. Define the responsibilities for the Information Technology (IT) Department and County Departments with DMV access

II. Definitions

A. Change Advisory Board (CAB) – A group of people that support the assessment, prioritization, authorization, and scheduling of changes. While the CAB is not expected to approve changes, their role is pivotal in advising whether a change should be approved. As such, the members of the CAB are expected to be experienced in both business and technology to point out any significant issues that a technical change could result in if not managed properly.

B. Incident Response Plan (IRP) – The County's internal security guide for addressing the seven stages of incident response: preparation, detection, analysis, containment, eradication, recovery, and post-incident activities.

III. Policy

A. Departments with DMV access are required to follow the State of California data sharing and data use Information Forms (INF) 1128 and INF 1130.
- INF 1128, Information Security Statement (ca.gov)
- INF 1130, Government Requester Account Application

B. Departments with DMV access must comply with the DMV Information Security Agreement (ISA) which is used by the DMV to audit agencies with DMV access. Failure to comply with established DMV information policies and procedures will result in termination of access for the user and/or all department users. In addition, users are not allowed to use the following items:
   i. Remote connections to DMV are not allowed to access DMV data.
   ii. Removable media (DVDs, CDs, memory cards, USB devices, and external hard disk drives, etc.) is not allowed to process, store, or transmit DMV data.
   iii. DMV data cannot be shared or sold to third parties.

C. IT does not review or monitor the use of DMV data. Ensuring proper use of DMV data is a responsibility of the departments with DMV access.

IV. Procedures

1. IT Department shall be responsible for the following:

A. IT will maintain an active directory group for DMV users to apply additional National Institute of Standards and Technology (NIST) guidelines

B. IT will administrate DMV access
   i. Add and term DMV access when forms are submitted by the department (NIST PS-5)
   ii. Administrate passwords for DMV access

C. IT will complete a security and risk assessment every six (6) months
   i. Conduct vulnerability scanning (NIST RA-3)
   ii. Review system firewall(s) and router configurations to identify and eliminate unnecessary functions, ports, protocols, and/or services (NIST CM-7)
   iii. Utilize the Change Advisory Board process for configuration management (NIST SA-10)

D. IT will sanitize and maintain equipment per DMV requirements (NIST MA-2)
   i. Designate personnel to approve the removal of department's information system components for off-site maintenance or repairs
   ii. Work with the department to ensure equipment is sanitized prior to removal for offsite maintenance for repair
   iii. Device maintenance records for department's information

E. IT will enforce system protections
   i. Implement cryptographic protection in storage and/or during transmission when requested by a department for DMV data (NIST SC-13)

F. IT will maintain Incident Response Plan (NIST IR-2, 6, 7, 8)

2. County Department with DMV Users shall be responsible for the following:

A. Establish an audit process per the audit and accountability requirements for DMV access for their department (NIST AU-3, 6, 9, 11)
   i. Create and maintain an audit log
   ii. Review audit log monthly
   iii. Keep the audit log in a secure location
   iv. Maintain a backup DMV audit records onto a system
   v. Retain audit information for a period of two (2) years from the date of the request

B. Establish DMV user procedures for their department

i. Require all individuals (employees, contractors, or agents) having direct or incidental access to DMV information to sign the Information Security Statement (form INF 1128) prior to authorizing access and annually thereafter (NIST PS-6)
ii. Require all DMV users to complete a DMV annual training and maintain record of completion for two years
iii. Submit a ticket to IT to request access removal from the DMV system if no activity after 60 days or within one week of employee termination (NIST IA-4)
iv. Retain the employee INF 1128 forms for a period of two (2) years after employee separation (NIST PS-8)

C. Use the Incident Response Plan (NIST IR-2, 6, 7, 8)

D. Establish data use and storage procedure for their department
i. Submit a ticket to IT when DMV data is being stored or transferred to ensure protection (NIST SC-13)
ii. Prevent unauthorized and unintended DMV information transfers via shared system resources (NIST SC-4)

IV. REFERENCES

US Department of Commerce National Institute of Standard and Technology (NIST) Special Publication 800-53 as noted.

V. RESPONSIBLE DEPARTMENT

Information Technologies and Participating Departments

VI. DATES (ADOPTED, REVISED, NEXT REVIEW)

Originally Adopted:	11/14/2023		
Last Revision:	11/14/2023	**Next Review:**	11/14/2027