INTRODUCTION

During each business day, DMV receives, processes, and distributes large volumes of information in the form of customer records and documents. Responsibilities relating to this information are given to DMV by the Code of Virginia, federal laws, and agency rules and regulations. The purpose of this policy is to ensure that all DMV employees and license agents are aware of their continuing responsibilities for the proper use and handling of DMV information, as well as the proper use of the information systems facilities and communication networks on which records are stored and processed.

This information is considered to be an asset and is to be protected because:

- Its accuracy is essential for the agency to carry out its programs.
- Other agencies use it to support their programs.
- Information concerning convictions is a record of court decisions and directions, and unauthorized alteration of these records is considered contempt of court as well as a violation of the Fair Credit Reporting Act.

Each of us in the Department of Motor Vehicles is affected in the performance of our duties by state and federal laws concerning unauthorized access, alteration, deletion and disclosure of information. These laws provide for safeguards concerning the information in citizen records and the information provided to DMV by courts, other state and federal agencies, other states, and private individuals and organizations. The laws also include provisions for civil and/or criminal prosecution and/or penalties for violators.

DEFINITIONS

The term “information” means all data, active and inactive records and documents, regardless of form, which are contained in or processed by the agency and its facilities to include license agents.

SCOPE

This policy applies to all agency information, information systems facilities and communications networks, and the records which they store and process.

The policy applies to all DMV employees, agents, and consultants and any person whose services to DMV are procured by a contract or through a temporary personnel agency.

The principal related statutes are:

- The Fair Credit Reporting Act (Public Law 91-508 of 1970 and its amendment of 1978, Public Law 95-598). This law details procedures which must be followed by consumer reporting agencies when disseminating to third parties such information as credit statutes, convictions, judgements and liens.
- The Freedom of Information Act (Code of Virginia 2.1-342). This statute opens agency records to the public, but requires agencies to ensure that policies and procedures are in place to review requests for information and deny release of protected and sensitive data.
- The Privacy Protection Act (Code of Virginia 2.1-377-386) requires certain procedural steps to be taken in the collection, maintenance, use, and dissemination of personal data.
- Release of Private Information statute (Code of Virginia 46.2-208 through 46.2-212 and other sections of state as well as federal statutes). Defines the information that DMV may disseminate and the specific information that various categories of persons and organizations may receive.
- The Virginia Computer Crimes Act of 1984 and its amendment of 1990 (Code of Virginia 18.2-152.1 through 152.14). Defines and provides penalties for various unauthorized actions, including invasion of privacy, which involve computers, computer networks, computer software, and financial instruments.
- The Virginia Public Records Act (Code of Virginia 46.1-76 through 46.1-91). Establishes a single body of law applicable to all public offers and employees on the subject of public record management and preservation and procedures, which are uniform on this subject throughout the Commonwealth.

RESPONSIBILITIES-LICENSE AGENT

License Agents have all the responsibilities described above as well as the following responsibilities relating to this policy and to the personnel that they employ:

1. Establish procedures, which address the specific duties performed in their agent, and which conform to this policy.
2. Ensure that your employees receive initial and ongoing training on the procedures for security of information. Provide specific job-related details to each employee, both verbally and in writing, concerning who may receive information, what information each party is authorized to receive, procedures for disposal of microfilmed documents which are no longer needed, and computer security procedures.
3. Ensure that your employees receive and continue to have the lowest level of access to automated records and source documents, which is necessary to perform the assigned work. DMV Select employees have the same level of access. For computer access, fill out the Extranet LogonID Request Form (US002) and send to the address on the form. Once this form is received a Fob will be issued. Use this form for the following situations:
   a. New or transferred employees.
   b. When your employee(s) have a change in duties: Review access level and initiate change if appropriate. (License agents only have one security profile).
   c. When an employee is no longer at the agent: Initiate access change when there is a transfer, promotion, resignation or other change in employment status. Note that you will continue to have security responsibilities for such employees until you initiate the change.
4. Supervise your employee's adherence to security policies to ensure that employees are logged off the DMV Select System when an employee leaves the area and that other procedures are followed.
5. Include adherence to security policies and procedures in the performance standards of those employees with access to confidential and personal information. This is only a suggestion for license agents.
6. Immediately report to your district manager or CSC manager any violation or suspected violation of security procedures.

RESPONSIBILITIES – LICENSE AGENT EMPLOYEES

License Agent employees will receive procedures for security of information and sign a form indicating receipt of these procedures. Employees will receive specific details, both verbally and in writing, concerning who may receive information, what information each party is authorized to receive, procedures for disposal of paper or microfilmed documents which are no longer needed, and computer security procedures.

License Agent Employees are responsible for adhering to the following guidelines:

1. Do not create, access, alter, delete, or release any records of the DMV except as necessary to perform your assigned duties.
2. Protect confidential and personal information to which you have access in paper, microfilm, or automated files by following all security procedures, such as keeping your password secret from all others, logging off your terminal, and locking up files when you are leaving the area.
3. Do not disclose customer information except when the Code of Virginia, the Fair Credit Reporting Act, and DMV rules, regulations, and operating procedures specifically allow it. This includes information from automated records as well as applications, attachments, and other documents gathered or created by the department concerning specifically identifiable individuals and private companies.
4. Request sufficient identification to assure yourself of the person's identity before releasing any customer information and before conducting transactions which will alter the records or affect an individual's status or eligibility for licensing or other departmental services.
5. Give confidential and personal information to another DMV employee only if that employee has an official need to know in connection with his or her duties.
6. Report immediately to your supervisor any knowledge you may have of a violation of this policy.
7. Safeguard information obtained through the National Criminal Information Network, The National Driver Register, CDLIS, or any other sources from disclosure to unauthorized parties in the same way that you safeguard information originating in Virginia.
8. DMV employees and license agent employees, like any other customers, complete an application and pay fees for personal transcripts and any other services of the department.

MANAGERIAL RESPONSIBILITIES

Persons at the district manager level have all the responsibilities described above. In addition, they are responsible for reviewing and approving all security access request forms prepared by subordinate supervisors to ensure appropriate security level assignments, and for maintaining a listing which is current at all times of all subordinate employees and their access levels.

ADMINISTRATOR AND EXECUTIVE RESPONSIBILITIES

Administrators and executives have all the responsibilities described above, and are ultimately responsible for consistent enforcement of this policy throughout their administrations or assigned areas of accountability. They usually also have delegated ownership authority and responsibility as described in "Responsibilities of Owners of Records and Systems."

RESPONSIBILITIES OF OWNERS OF RECORDS AND SYSTEMS

The Commissioner is the owner of all information originating in and housed in the Department of Motor Vehicles and its information systems. The Commissioner delegates ownership authority and responsibilities.

Owners have the following responsibilities:

1. To classify information by judging its value in terms of: a. whether it is governed by statute and b. whether it is sensitive.
2. To authorize access and modification.
3. To specify and enforce controls.
4. To communicate those controls to the custodian and users of the information.
5. To establish and administer retention schedules.

VIOLATIONS

Standard of Conduct and Performance

Under the Employee Standards of Conduct and Performance, violations of this policy may lead to dismissal. Unauthorized use or misuse of state property or information is a Group II or Group III offense. A second offense under Group II "normally warrants removal." A first offense under Group III may result in immediate removal.

Civil and Criminal Penalties

Most of the laws cited in this policy contain provisions for civil and criminal penalties. For example:

- Obtaining information under false pretenses, or unauthorized disclosure of information is punishable by a fine up to $5,000 or one year's imprisonment or both.
- Persons who are harmed may also bring civil suit for damages sustained, and the court may also award punitive damages, costs, and attorney's fees.
- Altering, erasing, or making copies of data is in some cases chargeable as a Class 6 felony.
- Unauthorized access or disclosure of another person's employment, salary, credit, or other personal or financial information is chargeable as a misdemeanor.

DMV requires that all license agent's and its employees must complete and sign the Information Security Policy and maintain a copy in the agent's files and submit the original to Department of Motor Vehicles, Customer Service Administration, Room 505, P. O. Box 27412, Richmond, Virginia 23269.

DMV CERTIFICATION OF RECEIPT OF INFORMATION SECURITY POLICY

As a DMV Contractual License Agent or an employee of a contractual license agent for the Department of Motor Vehicles, I certify that I have been informed of the Information Security Policy and I agree to adhere to its provisions as related to my position, which include but may not be limited to the following:

- I will not create, access, alter, delete, or release any records of the DMV except as necessary to perform assigned duties.
- I will protect confidential and personal information, whether on paper, microfilm, or computer files, by following security procedures as established by my assigned work area.
- I will not disclose customer information except when specifically allowed by the Code of Virginia, the Fair Credit Reporting Act, and DMV rules, regulations, and operating procedures.
- I will follow all identification procedures and requirements before conducting transactions which alter an individual's records or affect an individual's eligibility status for licensing or other Department services.
- I will disclose confidential or personal information to another DMV employee only if that employee has an official need to know in connection with his or her job duties.
- I will immediately report any knowledge of a violation of this policy to my immediate supervisor.
- I will safeguard information obtained through the National Criminal Information Network, the National Driver Register, CDLIS, and any other sources from disclosure to unauthorized parties.
- I will complete an application and pay appropriate fees for personal transcripts or any other services of DMV

I understand that my failure to comply with this policy may result in disciplinary action or termination. I also understand that I may incur civil penalties and/or criminal prosecution as noted in the Virginia Computer Crimes Act of 1987 and applicable state and federal laws.

LICENSE AGENT/OR
EMPLOYEE (S) OF AGENT SIGNATURE _____DATE_____

EMPLOYEE NAME (PLEASE PRINT)_____

SOCIAL SECURITY NUMBER _____