New Employee Orientation Policies and Procedures

www.dmvNow.com

SUPERIOR SERVICE | SECURE CREDENTIALS | SAVING LIVES

DMV. It's more than a job.

Welcome to new employee orientation. We are delighted you have joined the Department of Motor Vehicles (DMV). As you become familiar with DMV, you will discover this agency is not just another place to work, but a dynamic opportunity to serve the citizens of Virginia.

As part of your new employee orientation, this packet of information will help you learn more about DMV policies and procedures and online training requirements. All of these policies and procedures are posted on myDMV, (DMV's intranet) and can be easily accessed from a DMV computer.

During this orientation and throughout your DMV career, the Human Resources Office (HRO) is here to provide you with excellent service, benefits information and guidance. If you have any questions or concerns about your position, administration, benefits, or personal work-life issues, HRO has many resources available to help you. Just ask. We are happy to help you.

Table of Contents

e. Certification of Receipt of Information Security Policy Form (HRO 29) (1/20/2010)

Purpose: This form is used by DMV to certify that you have been informed of the Information Security Policy and have agreed to its provisions. This form is stored in your employee file and a duplicate copy is attached for your records.
Instructions: Read the requested information, sign and date the form. Your HR Consultant will collect the signed copy.
Completion Time Frame: During new employee orientation.

f. Internet and Email Usage Policy (Rev 2/2009)

Purpose: This policy is designed to establish guidelines for understanding the appropriate and prohibited usage of Internet and e-mail activities.

g. Policy on Outside Employment, Solicitation and Corporate Citizenship (Rev 10/2005)

Purpose: DMV employees are not allowed to engage in outside employment or pursue a business or professional opportunity with a business, organization or other entity that would present a conflict of interest with DMV. This policy differentiates between acceptable and unacceptable outside employment and also distinguishes between conduct that is prohibited and conduct that is permitted under the corporate citizenship program.

h. Policy on Telephone Services (Rev 1/2010)

Purpose: This policy reviews employees' permitted usage of telephone equipment, telephone lines, cell phones and pagers. This equipment is intended for official business use only and should be used in the most economical and secure manner possible.

i. Cell Phone Usage Policy (Rev 9/2011)

Purpose: This policy reviews employee's permitted use of DMV issued cell phones or any handheld electronic telecommunications devise with the ability to receive and/or transmit voice, text, or data messages without a cable connection.

j. General Safety and Security Policies (Rev 2/2009)

Purpose: DMV is committed to preventing injuries and maintaining a safe and secure working environment for all DMV employees. These policies address basic office safety tips, DMV's emergency evacuation plans, inclement weather closings or delays, employee identification badges and building access, and instructions if you receive a telephone threat.

II. Department of Human Resource Management (DHRM) and State Policies and Procedures

a. Policy Number 1.05 – Alcohol and Other Drugs (Rev 11/2006)

Purpose: It is the Commonwealth of Virginia's objective to establish and maintain a work environment free from the adverse effects of alcohol and other drugs. This policy addresses alcohol and other drug problems in the public work force and the disciplinary actions taken should an employee violate the policy.

b. DMV Supplemental Policy on Alcohol and Other Drugs (Rev 2/2012)

Purpose: This supplemental policy establishes requirements for DMV employees to notify their supervisors of any conviction relating to driving under the influence of alcohol or other drugs or refusing to submit to a blood or breath test either in or outside the workplace. This policy also outlines disciplinary actions that may be taken as a result of a conviction.

c. Policy Number 1.75 – Use of Electronic Communications and Social Media (Rev 3/2011)

Purpose: This policy addresses the appropriate and inappropriate use of the Internet and the state's electronic communication systems for state agencies and their employees.

d. DMV Supplemental Policy on Social Media

Purpose: Policy is a supplement to DHRM Policy on use of Electronic Communications and Social Media Policy and the purpose is to ensure the appropriate, responsible and safe use of electronic communications and social media by employees.

e. Policy Number 2.30 – Workplace Harassment

Purpose: This DHRM policy aims to educate employees about the recognition and prevention of illegal workplace harassment and to provide an effective means of eliminating such harassment in the workplace.

f. Policy Number 1.80 Workplace Violence

Purpose: To establish a procedure that prohibits violence in the workplace.

g. State of Virginia Grievance Procedure – (Non-Probationary Classified employees only)

Purpose: The Grievance Procedure gives employees an avenue to bring workplace concerns to the upper levels of management.

III. Required DMV Online Training

a. Acceptable Use Policy – User Acknowledgment

Purpose: This online training is designed to provide new employees with an overview of the acceptable use of Commonwealth of Virginia Information Technology resources.
Instructions: Review the instructions included in this packet to register, enroll, and complete the training through DMV Knowledge Center.
Completion Time Frame: Due within five days of employment.

b. Information Security Awareness and Training

Purpose: This online training is designed to provide new employees with training on how to be safe and secure in their use of Commonwealth of Virginia Information Technology resources.
Instructions: Review the instructions included in this packet to register, enroll, and complete the training through DMV Knowledge Center.
Completion Time Frame: Due within 30 days of employment.

c. Employee Code of Conduct Training

Purpose: Due to the nature of your work at DMV, your commitment to security, safety and service is required daily. This training will provide you with the tools needed to do your job effectively, professionally and adhere to the highest ethical standards.
Instructions: Review the instructions included in this packet to register, enroll, and complete the training through the DMV Knowledge Center.
Completion Time Frame: Due within 90 days of employment.

d. Terrorism and Security Awareness Training

Purpose: This online training is designed to orient employees on the subject of terrorism, provide basic self prevention and self protection techniques, and familiarize employees with their roles and DMV's role in responding to an emergency.
Instructions: Review the instructions included in this packet to register, enroll, and complete the training through the DMV Knowledge Center.
Completion Time Frame: Due within 90 days of employment.

e. DHRM-HR Policy – Alcohol and Other Drugs

Purpose: To promote the Commonwealth's objective of a work environment free from the adverse effects of alcohol and other drugs.
Instructions: Review the instructions included in this packet to register, enroll, and complete the training through the DMV Knowledge Center.
Completion Time Frame: Due within first 90 days of employment.

f. DHRM – HR Policy – Preventing Workplace Violence (for Employees)
Purpose: To establish a procedure that prohibits violence in the workplace.
Instructions: Review the instructions included in this packet to register, enroll, and complete the training through the DMV Knowledge Center.
Completion Time Frame: Due within first 90 days of employment.

g. DMV IT – Social Media Policy Training
Purpose: To ensure the appropriate, responsible, and safe use of electronic communications and social media by employees.
Instructions: Review the instructions included in this packet to register, enroll, and complete the training through the DMV Knowledge Center.
Completion Time Frame: Due within first 90 days of employment.

DMV Policies and Procedures

DMV Policy on Nepotism

Revision Date: 10/2005

Employees to Whom Policy Applies

This policy applies to (1) employees in positions covered by the Virginia Personnel Act, including fulltime and part-time classified and restricted employees; (2) non-classified employees in "at will" positions; (3) non-classified hourly (wage) employees; and (4) employees who are serving probationary periods.

Purpose

The State and Local Government Conflict of Interests Act (Code of Virginia 2.2-3100 through 2.2-3131) prohibits, as a conflict of interests, supervision by an employee of a member of his/her immediate family. In order to avoid the reality or appearance of improper influence or favoritism, DMV further prohibits supervision by an employee of any member of his/her family as well as an employee's participation in the selection process for a position if a family member is an applicant.

Definitions

"Immediate family" means (i) a spouse and (ii) any other person residing in the same household as the employee, who is a dependent of the employee or of whom the employee is a dependent. (Code of Virginia 2.2-3101).

"Dependent" means a son, daughter, father, mother, brother, sister or other person, whether or not related by blood or marriage, if such person receives from the employee, or provides to the employee, more than one-half of his financial support. (Code of Virginia 2.2-3101).

"Family member" refers to an employee's spouse, child, grandchild, parent, grandparent, brother, sister, niece, nephew, aunt, uncle or cousin, either by blood or by marriage. (For purposes of this policy only). "Supervise" refers to the authority to manage, oversee, hire, remove or discipline another employee or to exercise any control or influence over another employee's work or work activities. For purposes of this policy, an employee's reviewer or rater supervises such employee, as does an employee's work-leader, even if the work-leader does not rate or review the employee. (For purposes of this policy only).

Policy

- Code of Virginia 2.2-3106 prohibits, as a conflict of interests, supervision by an employee of a member of his/her immediate family.
- DMV further prohibits an employee from supervising or being supervised by any family member.
- DMV prohibits an employee from participating in the selection process for any classified, wage or contract position when the pool of applicants for the position includes a member of the employee's family. If this situation arises, the employee must disqualify himself/herself from the selection process for the position.
- In situations that do not involve a supervisory relationship, DMV recommends that an employee not be hired or transferred into a position that is located in the same Customer Service Center or work unit where any family member is employed.

Exceptions

A DMV employee who is currently employed with a family member in a situation that is permitted under the State and Local Government Conflict of Interests Act but is prohibited under this policy shall be allowed to remain in his/her current position. However, such employee will be subject to the terms of this policy if and when he/she is transferred or hired into any other position.

In extraordinary circumstances only, the Commissioner of DMV may grant an exception to this policy to permit an employee to supervise or be supervised by a family member who is not an immediate family member. This policy is not intended to permit a supervisoremployee relationship that is expressly prohibited under the State and Local Government Conflict of Interests Act.

Violation

An employee who willfully violates this policy may be subject to corrective action under the Department of Human Resource Management's Standards of Conduct. (Policy No. 1.60). In addition, the employee may be subject to penalties imposed by the State and Local Government Conflict of Interests Act.

Personnel Matters

Dress Guideline

Effective Date: 7/23/2007
Revised Date: 10/14/2015

Purpose:
To provide employees with general guidelines regarding appropriate dress for the workplace in an effort to present a business and professional image to our customers and business partners. This policy also provides general guidelines
on the displaying of tattoos and body piercings.

Applies To:
This guideline applies to all employees working at DMV, full-time and part-time classified employees, At-will, and wage (P14) employees. This guideline also applies to contractors, consultants and individuals working at DMV through temporary staffing agencies.

General Guidelines - Dress Standard

- The dress standard for the Department of Motor Vehicles is business casual. Business casual attire is clothing that allows employees to feel comfortable while working; however, the clothing should be appropriate for the work environment. Business casual attire encompasses many looks and includes various dress items such as: slacks, khakis, collared sport shirts, blouses/shirts, turtlenecks, sweaters, skirts/dresses, loafers. Employees may dress in more formal or traditional business attire if they choose (suits, shirt and tie, skirts/dresses, blazers/jackets).
- DMV expects that all employees maintain their appearance by ensuring they are clean, neat, and dressed appropriately for their job functions. DMV has a business casual dress guideline, but emphasizes that depending on the circumstances and work unit, there are times when individuals may be required to dress more formally for reasons such as meetings with external contacts.
- If an employee is conducting or attending meetings, seminars, conferences, etc. with other business professionals, he/she is expected to represent DMV in a professional manner and dress appropriately for conducting such business. Therefore, it may be appropriate for the employee to dress more formally. It is important for the employee to know his/her audience, remember that they are representatives of DMV and dress accordingly.
- Wearing of Jeans or similar type apparel:

  Employees working in mailroom and printing services are allowed to wear jeans as a result of the nature of the work performed.

  Managers may approve employees to wear jeans for a specific occasion such as work unit cleanup, moving, filing, etc.

  Employees are allowed to wear jeans when the agency has a delayed opening as a result of inclement weather and the Inclement Weather Policy is in effect.

  - Employees are allowed to wear jeans on **their last day of the work week (Fridays or Saturdays). This includes jean skirts, dresses, capri pants, and jackets**.

    Employees should not wear jeans if they are attending or serving as a representative at external meetings, workshops, conferences, training sessions, etc.

    Wearing jeans for any reason other than what is described above must be approved by management, and must be for a particular work activity for a specified time period.

Dress Standard - Building Maintenance and Weigh Stations:
Employees working in building maintenance and weigh stations are issued DMV uniforms. For more information, refer to the Work Unit Dress Guidelines and Uniform Policy.

Dress Standard - Enforcement & Compliance:
Employees working in the Enforcement and Compliance Administration such as Law Enforcement Officers may wear DMV issued uniforms which may include cargo pants. For more information, refer to the Work Unit Dress Guidelines and Uniform Policy.

Dress Standard - CSMA (Customer Service Centers and DMV Direct):
The customer service centers are located throughout the state, therefore the District Managers and CSC Managers may choose to apply more specific guidelines for dress and grooming based on the CSC and business needs. See the
CSMA Dress Guidelines for additional information.

Footwear

- Employees are allowed to wear athletic shoes (tennis shoes/sneakers). The athletic shoes should be clean, neat and not ripped or torn. Employees should use "good" judgment in determining the appropriate athletic shoes based on DMV's dress guideline and their individual work environments.
- Employees **are not** allowed to wear athletic footwear when meeting with vendors, contractors, etc., or if they serve as a representative for the organization at outside meetings, workshops, conferences, training sessions, etc.

General Guidelines - Dress Attire and Footwear Not Permissible:

- The DMV Dress Guideline has some specific clothing and footwear that are not appropriate for the workplace and, therefore, employees **are not** allowed to wear while at work. Such items include: jeans of any color (unless authorized as indicated in the Dress Guidelines); extremely loose or sagging pants; athletic apparel such as sports jerseys, sweat suits, jogging suits, wind suits, workout clothing; items that resemble lingerie, sleep wear, or beach wear; clothing that expose undergarments; revealing attire including plunging neckline blouses/shirts; leggjngs or jeggings worn without a dress or long length blouse/sweater.
- Employees are not allowed to wear beach flip flops/thongs/jandals, bedroom slippers/shoes, and athletic sandals/slide-ons while at work. Note: Please see chart at the end of this policy for additional information.

General Guidelines - Tattoos and Piercings
DMV is a customer service agency; therefore, it is important that the agency present a professional workforce that is customer friendly and appropriate. Consequently, the agency has set guidelines to address tattoos and piercings as detailed below.

Tattoos
DMV employees are not allowed to display tattoos, body art, or other body markings of any kind, specifically, from the waist up. Employees who have tattoos should make every effort to cover them while at work if possible. This includes fingers, hand, wrist and arm tattoos (gloves cannot be worn while working inside as a cover-up). In cases where tattoos cannot be covered or environmental and work conditions make it difficult to cover tattoos, employees may be allowed to work while displaying tattoos. In the case where tattoos are not covered, the visible tattoos must not be offensive (i.e. must not depict inappropriate or offensive words, symbols, pictures, logos, etc.). *(Example: An employee has a full sleeve tattoo and must conduct road test on a day when the weather conditions are extremely warm. The employee may be allowed to roll his/her sleeves up to keep cool.)*

Body Piercings
DMV strives to present a professional workforce at all times. Body piercings, just as tattoos, may also prevent a professional presentation. In addition, some piercings may be a distraction, as well as inhibit the ability to place the primary focus on the needs as communicated by the customer. Therefore, DMV employees are allowed to wear limited body piercings.

Piercing Guidelines:

Employees may wear ear piercings, no more than three on each ear;

Employees are allowed to wear one facial piercing. The piercing must be a stud, and 18 gauge in size or smaller;

Hoops piercing are allowed on the ears only. All other piercing must be a stud;

Nose piercings should be through the nostril. Piercings through the septum of the nose are not allowed.

Tongue, chin, and lip piercings are not allowed.

All other visible piercings, face or elsewhere on the body, must be removed while at work.

Agency Responsibility:

- Supervisors are responsible for the consistent application of this policy. Supervisors have the responsibility to counsel employees and make recommendations if this policy is not adhered to.
- If an employee reports to work and is found to be in violation of this policy, the supervisor should instruct the employee to leave work and report back to work appropriately dressed based on the dress guidelines. The employee will not be compensated for time away from work if he/she is asked to leave work as a result of inappropriate attire. However, the employee may utilize his/her leave for the time spent away from work.
- Violation of this guideline may lead to disciplinary action under the Standards of Conduct, Policy 1.60, or other appropriate action for contractors, consultants, and individuals working at DMV through temporary staffing agencies.
- DMV will make reasonable accommodations for dress or grooming directly related to an employee's religion, ethnicity, disability or medical needs. The employee may be required to present documentation to the supervisor and/or Human Resources for reasons related to disability or medical conditions.
- If an employee is not sure whether an article of clothing, tattoo, or piercing is appropriate for the workplace or have questions regarding the dress guidelines, he/she should confer with their supervisor or HR consultant.

General Practice:
The Dress Guideline is meant to offer a guide to employees in regards to appropriate dress and grooming in the

workplace. It is not the intent of the DMV management team to dictate clothing or other related physical appearance distinctions for employees. DMV promotes an environment that is professional and conveys service in every way to its customers and business partners. One of the ways that a professional environment is accomplished is through first appearances. It is understood that dress guidelines are subjective. Therefore, management staff asks that employees utilize good judgment and common sense as it relates to their professional appearance while at work.

Dress Guideline Quick Reference Charts:
The list below is a representation of appropriate and inappropriate attire.

Appropriate Attire
Dresses and skirts
Suits
Khakis/slacks Leggings/jeggins with a dress or long length blouse/sweater Capri pants *(Definition: Also known as capri, crop pants, long or three-quarter pants, and clam diggers; mid-calf pants usually worn in warm weather.)*
Shirts/blouses (collared and non-collared), DMV logo shirts
Sweaters and blazers
Casual shoes and sneakers (per guideline)
ONLY on the last day of the work week (Fridays or Saturdays) jeans, jean skirts/dresses/Capri pants and jackets.

Inappropriate Attire - Not Allowed
Miniskirts/dresses, jean skirts/jean dresses
Sweat suits/wind suits/jogging suits
Jeans of all colors, cargo pants, shorts
Leggings (including jeggings and similar pants) worn without a dress or long length blouse/sweater
Tube tops, halters, midriff and backless shirts Spaghetti-strap or strapless tops or dresses (worn without an appropriate covering shirt either on top or under attire)
Sports jerseys, t-shirts with inappropriate symbols, words, logos, etc.
Beach flip flops/thongs/jandals/shower shoes (*Definition: A type of waterproof open-toed sandal intended for use at the beach or poolside, made solely of plastic and/or rubber, and consisting of a flat or slightly elevated sole held loosely on the foot by a Y-shaped strap that passes between the first and second toes and*

Richard D. Holcomb, Commissioner

Information Security Policies — User Responsibilities

Revision Date: 02/16/2010

DMV Employees

Employees will be periodically required to officially review this policy. That review will be done to ensure that they are aware of their responsibilities for the security of information accessed, processed, or stored at or by the Department of Motor Vehicles (DMV). When employees are required to complete the policy review, they will use their DMV PIN to record that they have completed the review. An electronic record will be kept showing all employees who reviewed the policy. Employees will be able to print a certificate of completion as evidence of having reviewed the policy.

All DMV IT system users, including employees and contractors, shall be required to complete IT security awareness training annually, or more often as necessary.

Employees will periodically receive specific details, as needed for their job duties, about:

- Who may receive information,
- What information each party is authorized to receive,
- Computer security procedures, or
- Procedures for disposal of paper or microfilmed documents which are no longer needed.

Employees can access, review, or print this policy.

Employees of the DMV are responsible for adhering to the following, as well as specific policy components that relate to their job duties:

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 to in paper, microfilm, or automated files by following all security procedures, such as:
   - Keeping your password secret from all others,
   - Logging off your terminal or PC, and
   - Locking up files when you are leaving the area.
3. Do not disclose customer information except when the Code of Virginia, Federal laws, 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 (see Dissemination of Information on DMV's Intranet)
   - 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 records to another DMV employee only if that employee has an official need to know in connection with his or her duties.
6. Like any other customers, complete an application and pay fees for personal transcripts or any other services of the department.
7. Safeguard information obtained through the National Criminal Information Network, the National Law Enforcement Tracking System, 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. Report immediately to your supervisor any knowledge you may have of a violation of this policy.

Contracted Personnel

Contractors, consultants, vendors, and temps must adhere to the same responsibilities as DMV employees

and any information security requirements noted in the contracts their placement agency has with DMV.

Non-Employees

Volunteers and Interns must adhere to the same responsibilities as DMV employees when they serve in areas with access to information covered in this policy.

Personnel Who Supervise Others

Supervisors have all the employee responsibilities described above as well as the following responsibilities relating to this policy and to the personnel whom they supervise:

1. Establish and follow security procedures that address the specific duties performed in your area and which conform to this policy
2. Ensure that your employees, contracted personnel, and non-employees receive initial and ongoing training on the procedures for security of information and systems. 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 paper or microfilmed documents which are no longer needed, and
    - Computer security procedures.
3. Ensure that your employees, contracted personnel, and non-employees receive and continue to have the lowest level of access to automated records and source documents that is necessary to perform the assigned work. For computer access, please use the "System Access Request Form" in DMV Mini Forms. This form has a different version for Headquarters, for CSC's, and for Motor Carrier Service Centers.

Request the needed accesses on or before the effective date of the action for the following situations:

- New or transferred employees – Initiate or change access at the required level.
- Current employee with change in duties – Review access level and initiate change if appropriate.
- Employee is no longer under your supervision - Initiate request to remove access when there is a transfer or promotion.
- Employee resigns or is terminated – Initiate action to remove access.
- Employee who must be away from his or her job for an extended period of time without regular, remote access to DMV systems – Initiate action to suspend access.

4. Ensure that the access of your employees, contracted personnel, and non-employees is current at all times.
5. Supervise your employees, contracted personnel, and non-employees adherence to security policies to ensure that terminals are logged off when the employee leaves the area and that other procedures are followed.
6. Include adherence to security policies and procedures in the performance standards of those employees with access to confidential and personal information.
7. Immediately report to your management any violation or suspected violation of security procedures.

Executives and Management Personnel

Executives, administrators, directors, division managers, and district managers are considered supervisory personnel, but they are also responsible for consistent enforcement of DMV security policies and procedures throughout their administration or assigned areas of accountability.

Responsibilities of System and Record Owners

The Commissioner is the owner of all information originating in and housed in the DMV and its information systems. The Commissioner delegates ownership authority and responsibilities primarily to executives, administrators, directors, division managers, and district managers. Owners have the following responsibilities:

1. To classify information by judging its value in terms of:
    - Whether it is governed by statute,
    - 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.

Custodians

DMV's Information Technology Services (ITS) and the Virginia Information Technologies Agency (VITA) are the primary custodians of DMV's automated records and are responsible for the processing, storage, and control of DMV's computing resources. The custodian implements and administers controls over automated records as specified by the owners, or as deemed necessary by vendors or the custodian. Custodian responsibilities and procedures include:

1. Providing technical safeguards over: Databases & Interfaces, Network Connections, Security-related products, Hardware configurations, Internet configurations/accesses, Systems Architecture Documentation, Systems Software, and Application Software.
2. Providing physical safeguards, including access to HQ computer rooms, CSC computing resources, terminal logoffs, and PC Passwords.
3. Providing procedural guidelines for users of DMV computing resources, including: System Access Request Form and associated procedures, Non-disclosure agreements, and Internet Usage.
4. Administration and enforcement of DMV and third-party information security policies, procedures and access rules.

www.dmvNow.com
Virginia Department of Motor Vehicles
Post Office Box 27412
Richmond, Virginia 23269-0001

INFORMATION SECURITY POLICY ACKNOWLEDGEMENT

HRO 29 (11/25/2014)

Purpose: Use this form to acknowledge receipt of and compliance with the Virginia DMV's Information Security Policy.

Instructions: Give completed form to HR Consultant or HRO, Room 124.

EMPLOYEE INFORMATION	
EMPLOYEE NAME	EMPLOYEE DMV ID NUMBER
EMPLOYEE TITLE	EMPLOYEE DEPARTMENT/LOCATION

EMPLOYEE CERTIFICATION

As an employee of the Department of Motor Vehicles (DMV), 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 DMV records 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 that alter an individual's records or affect an individual's eligibility status for licensing or other DMV 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 Registry, 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 DMV services.
- I will complete the on-line Acceptable Use Policy - User Agreement Acknowledgment Training through the DMV Knowledge Center within 5 days of employment.
- I will complete the on-line Information Security Awareness Training through the DMV Knowledge Center within 30 days of employment.

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.

SIGNATURE	DATE (mm/dd/yyyy)

www.dmvNow.com
Virginia Department of Motor Vehicles
Post Office Box 27412
Richmond, Virginia 23269-0001

INFORMATION SECURITY POLICY ACKNOWLEDGEMENT

HRO 29 (11/25/2014)

Purpose: Use this form to acknowledge receipt of and compliance with the Virginia DMV's Information Security Policy.

Instructions: Give completed form to HR Consultant or HRO, Room 124.

EMPLOYEE INFORMATION	
EMPLOYEE NAME	EMPLOYEE DMV ID NUMBER
EMPLOYEE TITLE	EMPLOYEE DEPARTMENT/LOCATION

EMPLOYEE CERTIFICATION

As an employee of the Department of Motor Vehicles (DMV), 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 DMV records 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 that alter an individual's records or affect an individual's eligibility status for licensing or other DMV 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 Registry, 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 DMV services.
- I will complete the on-line Acceptable Use Policy - User Agreement Acknowledgment Training through the DMV Knowledge Center within 5 days of employment.
- I will complete the on-line Information Security Awareness Training through the DMV Knowledge Center within 30 days of employment.

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.

SIGNATURE	DATE (mm/dd/yyyy)

Information Security Policies — Internet and Email Usage

Revision Date: 02/26/2009

Policy

It is the policy of DMV to provide Internet and email access to DMV employees and other agency approved personnel. Agency-provided computer systems that allow these accesses are the property of the Commonwealth and are provided to assist in the effective and efficient conduct of State business. DMV users are permitted to use these accesses as an aid in the performance of their jobs.

Purpose

This policy is designed to establish guidelines for understanding the appropriate and prohibited usage of Internet and email activities.

Applies To/Scope

The requirements in this policy apply to all DMV employees, and agency approved contractors, agents, vendors and other personnel within DMV.

Procedures/Requirements/Standards

Valuable information supporting this policy can be found by clicking on these links.

- "Think Before You Click" (http://pscript/intranet/news/co_event.asp?anid=47) – Prohibited activities published by Communications Office.
- Employee Bulletin Board (http://pscript/dmvweb/bb/) – Use this for sharing personal information with others at DMV.
- Email Access (http://mydmv/intranet/manuals/general/emailaccess.shtml) – Facts you need to know about your email.
- Automatically Forwarded Email – No email will be automatically forwarded to an external destination without prior approval from the appropriate manager or director. Outlook is set up to reject rule generated messages going to the Internet. There are specific accounts such as "hearingreq" that are listed on the DMV web site to let customers know that their email was received.
- Spam Prevention (http://mydmv/intranet/administrations/its/nssspam.shtml) – Methods DMV uses to prevent receipt of unsolicited junk mail.

Authorities

Use of Internet and Electronic Communication Systems policy (DHRM Policy – 1.75) http://www.dhrm.state.va.us/hrpolicy/policy/pol1_75.pdf is the primary policy for all state employees to follow when using Internet and email.

DMV Policy On Outside Employment, Solicitation, and Corporate Citizenship

Revision Date: 10/2005

Employees to Whom Policy Applies

This policy applies to employees in positions covered by the Virginia Personnel Act, including full-time and part-time classified and restricted employees.

Purpose

DMV employees are prohibited from engaging in outside employment or pursuing a business or professional opportunity with a business, organization or other entity that is subject to DMV regulation, oversight or evaluation with a contractor, subcontractor, or vendor that conducts business with DMV. For purposes of this policy, outside employment includes ownership, in whole or in part, or other personal interest in such business, organization or other entity. In addition, DMV employees are prohibited from engaging in solicitation at work, and this policy distinguishes between conduct that is prohibited and conduct that is permitted under the corporate citizenship program.

Policy

Outside Employment, Business and Professional Opportunities

The following is prohibited conduct with regard to outside employment:

- Under no circumstances may DMV employees engage in outside employment or professional or business opportunities during the hours for which they are employed to work at DMV. DMV employees are not permitted to utilize sick leave in order to engage in outside employment or other professional or business opportunities. Similar restrictions apply to DMV employees claiming benefits under the Virginia Workers' Compensation Act, and such employees are subject to the rules established by the Virginia Workers' Compensation Commission governing concurrent (simultaneous) employment.
- DMV employees are not permitted to engage in outside employment or professional or business opportunities outside their work hours if such activity is deemed by DMV to affect the employees' work performance or to be in violation of the State and Local Government Conflict of Interests Act (Code of Virginia 2.2-3100 through 2.2-3131) or the Virginia Public Procurement Act, Ethics in Public Contracting provisions (Code of Virginia 2.2-4367 through 2.2-4377).
- DMV will not approve requests from a DMV employee to engage in an outside endeavor that involves payment for services rendered to, or employment in, a business, organization, corporation, firm or any other entity that is subject to regulation, oversight or evaluation by DMV or with a contractor, subcontractor or vendor that conducts business with DMV.
- DMV employees are prohibited from participating in a procurement transaction when certain types of connections exist between the DMV employee or a member of his/her immediate family and a bidder, offeror or contractor. These connections include a DMV employee's employment or prospective employment with the bidder, offeror or contractor; greater than 5% ownership or interest in the entity that is making a bid or offer or entering into a contract; and pecuniary interest in the transaction/personal interest in a contract.

  "Immediate family" means a spouse, child, parent, brother, sister, or any other person living in the same household as the employee. (Code of Virginia 2.2-4368).
- No DMV employee shall accept any business or professional opportunity when the employee knows that there is a reasonable likelihood that the opportunity is being offered to influence the performance of his/her official duties.
- No property belonging to or under contract to DMV may be used to conduct outside employment/business or professional activities.

Solicitation

For the purposes of this policy, solicitation is defined as asking for, offering or accepting any money or other thing of value in exchange for goods or services. Solicitation includes, but is not limited to, the distribution of catalogues or other commercial materials in an attempt to induce sales or to promote in any way a business or other commercial enterprise.

- Solicitation by DMV employees during work hours is strictly prohibited.
- Solicitation by DMV employees on DMV property, whether or not such solicitation occurs during work hours, is strictly prohibited.

Corporate Citizenship

DMV encourages employees to support and participate in civic, educational, cultural and other charitable causes and activities.

- DMV employees may engage in activities, including carrying out sales and eliciting donations, in support of charitable causes on DMV property, provided that they do not coerce others to contribute or otherwise participate. However, such charitable activities are permissible on condition that they do not involve raffles, contests or other games of chance.
- With prior approval and authorization, DMV employees will be permitted to engage in such activities during work hours.
- With prior approval and authorization, DMV employees may use DMV equipment and supplies - in moderation - for the benefit of such organizations and entities.
- DMV employees should direct questions to and seek authorization/approval for such activities from their managers or supervisors.

Procedures

Outside Employment, Business and Professional Opportunities

- DMV employees are required to notify DMV by submitting a written request for approval prior to beginning outside employment or pursuing an outside business or professional opportunity. The written request should be submitted to the employee's supervisor using form HRO 91. If an employee is already engaged in outside employment or is already pursuing an outside business or professional opportunity, such employee must submit his/her written request on Form HRO 91 immediately. The request must include the following information:
  - Employee name and identification number;
  - Outside employer/business or professional opportunity name and address;
  - Type of business/opportunity;
  - Duties to be performed;
  - Number of hours per week that will be devoted to outside employment/business or professional opportunity; and
  - Date employee intends to begin/began outside employment, business or professional opportunity
- DMV reserves the right to deny approval for any request should the agency determine that the outside employment/opportunity is in conflict with this policy.
- The DMV employee's supervisor will review the request, determine whether what is requested is appropriate under this policy and whether it is likely to interfere with work performance or attendance at DMV; and make a recommendation to the employee's DMV District Manager/DMV Director as to whether the request should be approved or denied.
- The supervisor will initial the Form HRO 91 to acknowledge its receipt and will forward the form, along with the supervisor's recommendation and any comments, to the DMV District Manager/DMV Director for consideration.
- The DMV District Manager/DMV Director will review the supervisor's recommendation and any comments provided for appropriateness of the employee's request under this policy and concerns about interference with work performance and/or attendance. The DMV District Manager/DMV Director will either or approve or deny the request on the Form HRO 91.
- The DMV District Manager/DMV Director will notify the employee of his/her decision in writing using a standard letter developed in conjunction with this policy. A copy of such letter and the original Form HRO 91 will be forwarded to the DMV Human Resources Office for inclusion in the employee's personnel file.
- If a conflict of interests arises after the employee's request has been approved or if it is later determined that the outside employment creates a conflict of interests or if an employee's work

performance or attendance suffers as the result of outside employment/pursuit of an outside business or professional opportunity, DMV reserves the right to withdraw approval for the request. This includes, but is not limited to, the situation where, after initial approval of a request, the outside business or other entity with which the DMV employee is involved either bids on or enters into a contract with DMV; in this situation, DMV will withdraw approval for the request.

- If an employee's request is denied or if approval for the request is subsequently withdrawn, the employee may appeal the decision to the Human Resources Office Director, who will have final authority to decide the matter.

Violation

An employee who willfully violates this policy may be subject to corrective action. Employees covered by the Virginia Personnel Act to include full-time and part-time classified and restricted employees may be subject to corrective action under the Department of Human Resource Management's Standards of Conduct. (Policy No. 1.60). In addition, the employee may be subject to penalties imposed by the State and Local Government Conflict of Interests Act.

Note: Even if DMV approves/authorizes outside employment or some other business opportunity, this action must not be considered an opinion or determination that there is no violation under the State and Local Government Conflict of Interests Act. If an employee has concerns or questions as to whether his/her outside employment or other business opportunity could possibly be a conflict of interests under the State and Local Government Conflict of Interests Act, he/she must seek advice from the Attorney General's Office to avoid prosecution.

Telephone Services

Revision Date: 01/2010

Policy

DMV telephone equipment, telephone lines, cell phones, and pagers are intended for official business only and should be used in the most economical and secure manner possible. See Usage of Services and Equipment.

Usage of Services and Equipment

- **Land Lines**

  Toll Calls:

  All calls that result in costs to DMV are subject to management review and approval. Telephone calls and the use of telephone equipment that result in costs to DMV are permissible only for Official DMV and State use.

  DMV Business Calls:

  VITA provides long distance telephone service through state contract providers. DMV lines are set up to route long distance calls by dialing 1 + the area code and number over the state contract provider's network. Overriding this dialing protocol by using the access codes of other long distance providers, such as dialing 10-10-220, etc., will result in a higher cost to DMV and is **not permitted**.

  Personal Use:

  Local Calls – Office practices govern the use of DMV landline telephones and equipment for making and receiving personal local calls.

  Long Distance Calls – Personal long distance calls on a DMV telephone landline are permitted after obtaining management approval under the following circumstances. The employee shall:

  Charge the call to the employee's home telephone;

  Reverse the charges, (calling collect);

  Charge the call to the employee's personal telephone credit card.

- **Modem Lines**

  Due to security concerns, modems and modem lines cannot be used in conjunction with a Local Area Network (LAN) connected to a PC. Exceptions to this policy must be requested in writing by the requestor (via E-mail or approval memo) and submitted along with an explanation for the conditions that warrant this exception. Requests for exceptions should be directed to DMV's Network Manager.

- **Cell Phones**

  All calls **to and from** a cell phone generate airtime charges to the cell phone account. This includes both local and long distance calling. Therefore, cell phones are to be used only when a landline is not available and only for reasons associated with DMV business.

  Cell phone account holders will be assigned either a flat rate account that charges for each minute of usage or a 200-minute block plan based upon anticipated usage. Initially, anticipated usage is derived from the account request justification and the purpose for which the cell phone is assigned. VTS is then responsible for tracking each account holder's monthly cell phone usage and making changes to the block plan as appropriate to ensure the most economical block plans are utilized.

  Most DMV cell phone accounts are maintained at the 200-minute block plan level. Increases to block plans at higher levels require authorization and justification from the appropriate assistant commissioner. As with any call that generates costs, managers are responsible and accountable for monitoring employee usage of accounts and certifying that usage is within DMV policy and guidelines.

- **Pagers**

  Pagers are provided for DMV business use and are intended solely for business purposes. The account holder's manager must authorize using a DMV pager to send and/or receive personal messages or pages that incur no charge to DMV. Two-way pagers or any pager that incurs usage charges must be used solely for business purposes. Monthly usage charges must be reviewed and certified by the manager or designee.

Violations

Violations of this policy will be addressed under DHRM Policy 1.60, Standards of Conduct. The appropriate level of disciplinary action will be determined on a case-by-case basis by management, with sanctions up to or including termination depending on the severity of the offense.

Reference

- Department of Information Technology Policy & Procedure Manual: Use of DIT Telephone Facilities, effective 6/16/92, revised 4/1/97.
- Department of Human Resource Management (DHRM) Policies and Procedures Manual, Use of Internet and Electronic Communication Systems, Policy number 1.75, effective date 08/01/01. Related Policies: DHRM Policy 1.60, Standards of Conduct and DHRM Policy 6.10, Personnel Records Management.

Responsibility

Virginia Information Technologies Agency (VITA) is responsible for the management, coordination, development, installation and use of all telecommunications facilities and services throughout the Commonwealth.

Purchasing or Contracting for Equipment and Services Policy

ITS/Voice Technology Services (VTS) receives and manages all DMV requests for voice telephone service including ordering and purchase, installation, relocation, repair and removal of telephone service, telephone sets, line service, modems, cellular phones, and pagers. See Requesting and Receiving Service or Equipment.

Management Responsibility for Equipment, Services, and Usage

DMV managers and employees to whom equipment and telephone accounts are assigned are **responsible** and accountable for ensuring that equipment is safely maintained, and that all usage is in accordance with agency and state policy guidelines. See Verification and Certification Procedures.

Responsibility for Returning Equipment/Requesting Termination of Services

Managers are responsible for retrieving and returning equipment, accessories, and requesting disconnection of assigned services upon transfer, resignation, or termination of employees under their supervision. See Procedures For Returning Equipment And Disconnecting Services.

Responsibility for Verification and Approval of Telephone Bill

Management or their designees are responsible for monthly review and approval of long distance charges, cell phone usage charges, two-way pager usage charges, and recurring line or circuit charges for equipment assigned to their cost codes. Managers should obtain justification from their employees when irregularities are found in long distance, cell phone, or two-way pager charges. Errors or changes in line assignments, cost code assignment, and inaccuracies in billed information must be reported to VTS for resolution and correction. See Verification and Certification Procedures.

Account Holders' Responsibility for Equipment, Services, and Usage

DMV employees to whom equipment and accounts are assigned are responsible and accountable for ensuring that equipment is safely maintained, and that all usage is in accordance with agency and state policy guidelines. See Usage of Services and Equipment.

Replacement cost of equipment due to loss, careless handling, or failure to return equipment upon resignation, termination, or transfer will be incurred by the employee. See Equipment Loss Procedures.

Equipment Assignment Policy

In order for employees to be accessible while they perform their work, they may request managerial approval for a cell phone or a pager, but not both. If an exception to this policy is warranted, and more than one wireless device is requested by the employee, the request for review and approval, including justification,

is to be directed by the requestor to the Agency's Executive Staff member responsible for Information Technologies.

Requesting and Receiving Service or Eqipment

Requestor

All requests for new telephones, cell phones, pagers, related equipment, or changes in services for such equipment must be approved and directed through Voice Technologies Services for processing and coordination with VITA or other vendors.

Request new telephone services, cell phones, pagers, related equipment or changes in services for such equipment through the appropriate manager, district manager or administrator, and include the following information:

- Description of equipment desired and/or work to be performed;
- Justification and business need for the expenditure. Justification for cell phone account must include how cell phone will be used and anticipated monthly usage.
- Location of telephone (room and floor number or Customer Service Center name or other DMV location);
- Telephone number if one has been assigned;
- Cost code to be billed;
- Features needed (ring-over, call pick up groups, voice mail, et cetera.).

Manager/Administrator/District Manager

- Review request;
- Determine whether business need justifies expenditure;
- Determine if budgeted funds are available;
- If approved, forward approval to VTS;
- If not approved, notify requestor
- Provide names of employee(s) designated to approve the monthly bill.

Note: VTS keeps a small inventory of cell phones and pagers for lending. If the need for a cell phone or pager is short term or incremental and does not justify the expense of purchasing the device and opening a permanent account, management should consider requesting a loaner cell phone or pager from inventory.

VTS

Receive request.

- Contact requestor to resolve any unclear items and to complete site survey if needed;
- For Cell Phone assess estimated usage and determine appropriate account plan;
- Advise requestor and requestor's manager of assigned plan.
- Contact telephone vendor for cost of wiring and jacks, and installation date;
- Complete MISA23 "Telephone Work Orders Log";
- Complete "Telecommunications Service Request" (VITA on-line form);
- Receive VITA acknowledgement and due date for request by fax or mail;
- Add VITA acknowledgement of requested service date to MISA 23, "Telephone Work Orders Log";
- Notify requestor by E-mail when the work is scheduled;
- Coordinate installation or change, instruct user on use, features, fully test lines and equipment;
- Update VTS database and Telephone Bill Application with appropriate information;
- Verify completion of service requested and customer acceptance;
- Order complete: Note completion date on MISA 23, "Telephone Work Orders Log" and file completed request;
- For new phone lines, cell phone, or pager accounts provide copy of telephone policy through the reporting manager;
- Order not complete: Contact requestor with new service date as agreed upon with service personnel.

Reporting Manager

- Counsel account holder on telephone policy, have employee sign receipt of Policy Confirmation Form.
- Forward signed policy confirmation to personnel office.

Verification and Approval Procedures

Policy

Recurring, Usage, and Long Distance Charges

Telecommunications bills from VITA will be distributed throughout DMV using the Intranet and the Automated

Telecommunications Billing Approval System (ATBAS). Management has designated employees to act as Approvers for specific cost codes who will have access to ATBAS in order to review and authorize the bills for payment within a set timeframe that must be met. The ATBAS will be implemented in September 2004.

Monthly recurring charges for individual telephone lines, including fax and modem lines, must be reviewed and verified by the Approver.

Monthly long distance charges from telephone numbers in each cost code must be reviewed and verified by the Approver each month.

Monthly cell phone use and pager use charges must be reviewed and verified by the account holder each month. The Approver for that cost code must then review the bill and approve it for payment.

Procedures

FMS (monthly)

- Distributes monthly telephone, cell phone, pager bills to Approvers and individuals via ATBAS.
- Receives approval of monthly telephone, cell phone, pager bills through ATBAS.
- Runs Exception reports, and follows up on unapproved bills.
- Co-administers telephone bill approval database with VTS.
- Pays all telecommunications invoices and follows up with any unapproved cost codes.

Approvers (monthly) upon receipt of bill with call detail information:

- Evaluate bill, reviewing long distance charges for time of day, repetitive calls to the same number, and appropriate usage according to business needs.
- Verify long distance, cell phone and pager use as in accordance with DMV and State policy.
- Coordinate corrective action with HRO to eliminate abuses and unauthorized use of telephone lines and equipment.
- Report inaccurate information or changes needed as an exception during the ATBAS process.
- Certify verification and approval to pay the bill.

ITS/NSS/VTS

- Confirm receipt of (TELREQ).
- Prepare Official Government Telecommunication Service (OGTS) form to send to VITA with information required to correct or change billing information.
- Make necessary updates to VTS database.
- Provide feedback to manager that change has been submitted to VITA and give effective date.
- Verify change on next bill.

Procedures for Reporting Problems and Requesting Repair

Requestor

To report problems with service and/or request repairs contact the VITA Customer Care Center (VCCC) at 1-866-637-8482 (if possible) or via Informs Network Support Center Problem Sheet (POINT) providing:

- Description of equipment,
- Location of telephone (room and floor number or Customer Service Center name and location),
- Telephone number,
- Cost code,
- Description of problem

NSC will try to troubleshoot the problem and may be able to resolve it immediately. If immediate resolution is not possible NSC will coordinate the repair with VTS.

ITS/NSS/VTS

- Begin resolution efforts within one hour after the problem was reported to NSC.

Telephone Lines and Sets, Cell Phone, Pager Return Upon Transfer or Termination

Managers

Upon employee reassignment, transfer, or termination-

- Recover cell phones, pagers, all accessories and return to VTS by date of move or termination.
- Request disconnection of services and termination of accounts using InForm TELREQ.
- Request disconnection of telephone, modem lines using InForm TELREQ and return telephone set to VTS.

Note: Reassignment or handoffs of equipment to other employees MUST be done in accordance with policy and coordinated through VTS.

Employee

Upon reassignment, transfer, or termination -

- Surrender cell phones, pagers, all accessories to your supervisor or manager by transfer or termination date.

VTS

Within two business days of receipt of InForm TELREQ or physical equipment (telephone sets, cell phones, pagers and accessories) -

- Take appropriate action to disconnect or reassign telephone lines.
- Return telephone set to inventory.
- Take appropriate action to terminate cell phone and pager accounts.
- Return cell phones, pagers, and accessories to inventory.
- Make updates to VTS database.

Violations: Violations of this policy will be addressed under DHRM Policy 1.60, Standards of Conduct. The appropriate level of disciplinary action will be determined on a case-by-case basis by management, with sanctions up to or including termination depending on the severity of the offense.

Procedures For Returning Equipment and Disconnecting Services

Manager

- Send request to disconnect service (Inform "TELREQ") within five business days of the transfer, resignation, or termination of an employee.
- Complete and print Equipment Return Form.
- Collect and return equipment, accessories, and completed Equipment Return Form to VTS, room 211, 2300 West Broad St., Richmond, VA 23269.

VTS

- Provide receipt form to Manager for returned equipment.
- Check equipment to ensure it is in working order.
- Make changes to databases to reflect return of equipment and deactivation of account.
- Return equipment to inventory for re-assignment.

Equipment Loss Procedures

Employees are responsible for the safeguarding of equipment provided to them by DMV. Loss of equipment through negligence will be the responsibility of the employee to which the equipment was issued. Please follow these procedures when any piece of telecommunications equipment (cell phone, pager, et cetera.), is lost.

Manager

- Notify VTS in writing of the loss of equipment and the circumstances under which it was lost. Include the type of equipment (cell phone, pager, etc.), the associated phone number (if applicable) and the employee's name.
- If desired, order new equipment by following procedures for Requesting and Receiving New Service or Equipment
- Any change in equipment must be adjusted on the work unit's "Controlled Assets Inventory."

VTS

- Notify FMS of equipment loss including cost of equipment
- Update VTS database to note loss of equipment
- Order new equipment upon receipt of request
- If the employee is resigning/terminated, notify FMS/Payroll if any equipment has not been returned, including the cost of the equipment.

FMS/Asset Management

- Make any adjustments necessary to asset management records.

FMS/Payroll

- Deduct the amount of any outstanding debt to DMV from the employee's last pay.

Cell Phone Usage Policy

Original Date: 09/23/2011

This policy must be reviewed and adhered to by employees authorized to use state owned cell phones, and their managers. Careful monitoring of usage allows the agency to more proactively manage their cell phones. The information below can help employees understand the terms of DMV's cell phone usage policy and users' accountability, thereby better managing telecom costs. Review the entire policy before requesting a cell phone.

Introduction

For the purpose of this policy, the term "cell phone" is defined as any handheld electronic telecommunication device with the ability to receive and/or transmit voice, text, or data messages without a cable connection (including, but not limited to, blackberries, cellular telephones, digital wireless phones, radio-phones, pagers, personal digital assistants with wireless communications capabilities (PDAs), or Research in Motion (RIM) wireless devices.

Section 1: Use of Cell Phones or Similar Devices

Use of DMV issued cell phones are specifically for business use only. **All** calls **to and from** a cell phone generate airtime minutes to the cell phone account. Therefore, cell phones are to be used only for reasons associated with DMV business. Most DMV cell phone accounts are maintained at the 200-minute block plan level. Increases to block plans at higher levels require justification and must have authorization from the appropriate assistant commissioner.

Personal Use of DMV Cell Phones

Personal calls are not allowed to be made on a DMV issued cell phone. Cell phones are to be protected by the employee, and returned to his or her manager when the need for the phone no longer exists or his or her employment ends.

Processing of the Request

- Requestor submits a cell phone account request and justification to his or her manager in writing.
- Manager submits a cell phone request using the TELECOMMUNICATIONS WORK ORDER in Secure Apps with the following information:

  Anticipated usage

  Purpose for which the cell phone is assigned
- If funding is available, the request is forwarded to the appropriate assistant commissioner for consideration of approval. **Approval from the appropriate assistant commissioner is required prior to the issuance of a cell phone. Blackberries are approved by the Deputy Commissioners.**
- Once approved, Budget Services will notify the employee, manager, and appropriate assistant commissioner of the cell phone number and details of the plan.

Review of Monthly Charges and Responsibilities of Managerial Staff

- DMV employees issued cell phones are accountable for their own cell phone use.
- Managers are responsible for monthly review and certification of use and charges for cell phone equipment assigned to their cost codes.

Monitoring

- DMV monitors usage of cell phones issued to employees. DMV has the right to monitor all cell phone usage. Monitoring may occur at any time, without notice and without the user's permission.
- Plans may be changed based on usage. In such cases, the employee and manager will be notified.
- Overages will be reported monthly to the appropriate assistant commissioner for review.

Section Two: Standards of Conduct

All employees must comply with this policy and any additional policies that may be adopted by this agency.

Violations

Violations of this policy will be addressed under Policy 1.60, Standards of Conduct. Employees will be responsible for unauthorized charges. Disciplinary action will be determined on a case-by-case basis by an employee's manager, Human Resources and/or the appropriate assistant commissioner.

General Safety Policies

DMV's Safety Objective

Regardless of your job, there are some basic safe work practices that should be observed by everyone. The objective of the DMV Safety Program is to prevent injuries and to allow you to do your job in a safe and comfortable working environment. Employees who follow a few simple workplace safety rules will minimize everyday hazards.

Basic DMV Office Safety Tips

- Turn off all electrical appliances when you leave work.
- Use only approved extension cords provided by Facilities Services and limit use in your work area.
- Never bring space heaters or coffee makers from home into the workplace. Only approved space heaters and coffee makers are allowed.
- Avoid storing materials in front of electrical panels, aisles and other points of egress.
- Immediately clean spills and other slip hazards found on floors.
- Use caution when walking on paved and tiled areas during inclement weather.
- When lifting anything, use the power of your legs and not your back.
- Be familiar with the emergency evacuation plan for your facility.
- Be familiar with the building layout and exit points.
- Immediately report any safety hazards to management.
- It's important to stay alert and to continuously be aware of your surroundings.
- Recognize suspicious activity by utilizing good judgment.
- Be familiar with the DMV Threat Report and ensure you have a copy by your telephone.

DMV Emergency Evacuation Plans

Customer Service Centers (CSC) and Motor Carrier Service Centers (MCSC)

- Evacuate the CSC/MCSC by calmly announcing over the intercom that there is a problem in the building and all employees and customers need to exit the building immediately.
- Designate key employees to assist customers in exiting.
- If you can do so without endangering yourself or others, secure all assets (monies, decals, titles, etc.) in a safe and spin the dials.
- Direct employees and customers away from the building and gather everyone at the pre-identified Evacuation Assembly Area.
- Any time police or fire personnel at the scene give instructions or suggestions, they are to be followed immediately.
- Post one management person near the door in a safe place to make sure no one re-enters the building.
- CSC's – Contact your district manager – if no one answers, contact the CSMA Administration at (804) 367-1858.
- MCSC's – Contact your regional manager – if no one answers, contact the MCS Administration at (804) 367-0040.

Complete a DMV Incident Report after the emergency is over and forward the original to your district manager, forward copies to the LES Director, CSMA/MCSO Director, FSPA Emergency Operations Manager. Also, retain a copy for the CSC/MCSC.

Headquarters Building (Alarm Conditions)

- Remain calm.
- The fire alarm warning devices will sound and the strobe lights will flash.
- A voice will advise you to either evacuate the building or stand-by.

People on the effected floor and the floor above and below will be told to evacuate.

People in the remainder of the building will get the stand-by message.

- If you are told to evacuate:

  Immediately head to the nearest emergency exit.

  Exit the building and report to the evacuation assembly area (The heliport next to H Lot).

- Follow the instruction of the Fire Wardens and DMV officials and do not leave the area or reenter the building until you are instructed.
- If you are told to stand-by:

  Prepare yourself to leave the building. (Shutdown your PC, get your car-keys, get your coat, etc.)

  Do not change floors or use the elevators or stairs until you are told to evacuate.

- If you have physical limitations that render you unable to utilize the stairs:

  Remain calm.

  Go to the elevator lobby on your floor.

  Take any of the normal elevators to the first floor. (Do not use the elevators if you are able to descend the stairs).

  The elevators will remain functional during a fire alarm as long as it is safe for them to operate.

  Exit the building and report to the evacuation assembly area (The heliport next to H Lot).

  Follow the instruction of the Fire Wardens and DMV officials and do not leave the area or reenter the building until you are instructed.

Inclement Weather Closings or Delays

In accordance with the Department of Human Resource Management (DHRM) Policy 1.35, Emergency Closings, for administrative state agencies in the city of Richmond, Chesterfield, Hanover, and Henrico counties, the Governor or his designee shall make closing decisions about the daytime hours of administrative agencies when conditions affect more than one administrative agency. DHRM will announce the Governor's decisions about authorized daytime closings of administrative office through television and radio stations. For closing information for agencies in the Richmond-Metro area you can:

- Listen to WRVA radio (1140 AM) or any Clear Channel affiliate (Q94, Lite 98, XL 102, 106.5, Sports Radio 910).
- Watch local television stations WTVR (6), WRIC (8), and WWBT (12).
- Visit DHRM's web site at www.dhrm.state.va.us and read the general policy about emergency closings.
- Call the Highway Helpline at 1-800-367-ROAD.

For DMV employees who work outside the Richmond area, your District Manager is designated to make closing decisions. You will need to follow their procedures for announcing decisions about authorized closings of the offices or facilities in your particular district or region.

Telephone Threat

The likelihood of you ever receiving a bomb or other threat is remote. However, if it should happen there are certain things you need to keep in mind:

- Remain calm and be courteous.
- Write down the caller's number from the phone display screen.
- Keep the caller on the line as long as possible by asking questions from the Threat Report form (IS 98). Complete as much of the form as you can while the caller is on the line. The investigating police officer will review the threat report with you later during the course of the investigation.
- Listen very carefully. Ask the caller to repeat himself if you did not hear or were unable to write down what he said.
- If possible, get a second employee to listen to the caller.
- Pay attention to background noises on the caller's end of the line.
- After the call is completed, call the authorities from a different phone using the numbers listed above.
- Dial *69 if you did not get the caller's number. Dialing *69 will not connect you to the caller, but depending on your telephone, it may give you the caller's number by computer-enhanced voice or by display on your telephone monitor.
- Review the information you recorded to ensure that it is complete and accurate.

IS 98 (04/02)

DEPARTMENT OF MOTOR VEHICLES
OFFICE OF THE INSPECTOR GENERAL

THREAT REPORT

Date: _____ Time call began _____ Time call ended _____

Caller's name: _____ Caller's phone #: ( ) _____

Telephone # on caller id: ( ) _____

Caller's exact words*: (use back if needed)*

BOMB THREAT	OTHER THREAT
Where is it? _____	Type of threat? _____
When will it go off? _____	What is threatened? HQ/CSC/Other?
What does it look like?: _____	
What will cause it to explode?	Person threatened?
Why did you set it?	Why are you upset?

Check Information

Caller	☐Age_____	☐Male	☐Female	☐Adult	☐Juvenile
English language	☐Good	☐Poor	☐Vulgar	☐Slang	☐Broken
Accent	☐Local	☐Not Local	☐Foreign	☐Identify _____	
Voice tone	☐Loud ☐Pleasant	☐Soft ☐Slur	☐High Pitch	☐Deep	☐Raspy
Speech pattern	☐Fast	☐Slow	☐Nasal	☐Lisp	
Manner	☐Calm ☐ Not understandable	☐Angry	☐Rational ☐Deliberate	☐Irrational ☐Emotional	☐Laughing ☐Other
Background noise	☐Noisy ☐Airplane ☐Animal	☐Trains ☐Factory ☐Quiet	☐Traffic ☐Voices ☐Office	☐Harbor ☐Ocean ☐Tv	☐Music ☐Party ☐Radio
Voice Familiar?	☐Name :		☐ Place familiar:		

Other information you feel is important*: (use back if needed)*

Did You Use?: ☐ MCT (Malicious call trace?) ☐ Recording device? ☐ *57 ☐ *69 ☐ Other *(see remarks)*

Remarks:

Person taking call: *print full name*	Phone number:	Your work area:

Headquarters employees should call Security at 367-6716 or 367-0468; field employees should follow their normal emergency procedures and/or dial 911 first and then contact their ISO district special agent in charge.

DEPARTMENT OF MOTOR VEHICLES
OFFICE OF THE INSPECTOR GENERAL

THREAT REPORT

ADDITIONAL INFORMATION

Become familiar with the form and information

The likelihood of your ever receiving a bomb/other threat is remote. However, if it should happen there are certain things you need to keep in mind: **1.** Remain **calm**. **2.** Be **courteous**. **3.** Keep the caller **on the line** as long as possible. **4. Listen** very carefully (ask the caller to repeat if you did not clearly hear what was said or failed to write down what was said). **5. Do not interrupt** the caller. **6.** Try to get **another employee to listen** in on the call. **7.** Pay attention to the **background noises**, (i.e. motor running, train, music, TV, radio, etc). **8. Call the authorities**. **9.** While waiting for help, **review** the threat report and add information you may have missed. **10. Record** your information accurately.

A calm response to the threat caller could result in obtaining additional information. This is especially true if the caller wishes to avoid injuries or deaths. If told that the building is occupied or cannot be evacuated in time, the bomber may be willing to give more specific information on the bomb's location, components, or method of detonation. If you have a recording device, do not rely on it totally… take notes and complete the threat report.

Note: MCT (malicious call trace) and recording devices are not available on every telephone. Dial *57 immediately after the caller hangs up. *57 will record the callers telephone number, but the number can only be retrieved by law enforcement. Dial *69 immediately after the caller hangs up, however, *69 does not work on all telephones. Check your telephone book for other services not noted.

General Security Policies

Employee Identification Badges and Headquarters Access Cards

DMV requires a photograph to be displayed on employee identification cards. All headquarters employees are also issued building access control cards which allow them access to various parts of the building and their assigned parking lots. All cards are the property of DMV and employees are responsible for safeguarding them at all times.

Lost or misplaced cards can be replaced for $5.00. To receive an employee ID, complete a Consent to use Driver's License Photograph on Employee Identification Badge form (HRO 32).

All employees must wear their DMV employee ID so it's always visible. For example, you may clip your ID to the outside of your clothing or wear it on a light cord around your neck, outside of your clothing. If you need clips or cords, contact Human Resources in Room 124 at headquarters.

All employees are required to display their ID card as they move throughout the building. The ID/access cards must be presented each time an employee enters a service area, including after lunch, breaks, or after leaving and returning to the building.

When entering headquarters:

- All employees are required to have and display their employee ID for building access.
- Visitors are required to sign in at security and be escorted to designated building areas.
- Long-term service contractors should have completed criminal background checks and display photo identification cards while working in the building.
- Short-term service contractors are to be escorted to building areas.

Headquarters Building Access

Normal Working Hours

- During normal working hours, all employees who enter the front and rear entrances of the building to access the stairwells, elevator areas and non-public areas of the building through the first floor or basement areas, will be required to present their ID card and utilize their access card to gain access to these areas.

  If an employee's access card fails to work properly, the employee's supervisor/manager will be contacted for authorization to give the employee access to non-public areas. The supervisor must also notify Human Resources Office to reprogram/reissue the employee's access card.
- All employees are required to display their ID card as they move throughout the building. The ID/access cards must be presented each time an employee enters a service area, including after lunch, breaks, or after leaving and returning to the building.
- In the event that the employee does not have his/her access card, the employee will report to the security desk. Security will then contact the employee's supervisor/manager and request that they grant permission for the employee to have access to the building. Upon authorization by management, security will issue a temporary pass. After obtaining the temporary pass, the employee will be required to immediately move his vehicle from the customer parking lot to their assigned lot. Failure to move the vehicle will be considered a parking violation. The temporary pass must be returned to security at the end of the employee's shift.
- All visitors, agency guests, and non-employees not having a DMV ID card will be required to obtain a visitors pass from security. Security will contact the person to be visited. A visitor's pass will then be issued. The DMV employee will come to the first floor security office and escort

visitors to all non-public areas. The visitor's pass must be visibly displayed on the individual visitor's clothing for the duration of their visit.

In the event of a pre-scheduled meeting, the meeting coordinator will provide the security office with an advance list of persons approved to enter the building for the meeting. The list should include the approved individuals' names, along with the date, purpose of the meeting and location of the meeting and parking information.

- Visitors, agency guests, or other non-employees must return the visitors passes to the first floor or loading dock security office and sign-out upon completion of the authorized visit.
- Other visitors (such as relatives of employees, friends of employees, or former employees) must enter the front lobby and sign in at the security desk for a visitor pass. They may not access non-public areas (work areas above the first floor) without an escort and authorization from the supervisor of the area to be visited.

  These types of visits should be of a reasonable length of time (example: employee's break or lunch period) and should be limited to the employee's work area in which the visitor was originally authorized.

<u>After Hours Building Access</u>

- Entrance to the building after normal work hours, on weekends and holidays will be limited to DMV employees with valid ID/access control cards and their authorized escorted guests.
- Employees entering the building after hours must stop at the security desk, show their DMV ID, sign-in on the after-hours log, and proceed only to their work area.
- Employees exiting the building after hours (6:30 p.m.) Monday through Friday, must sign out on the after-hours log at the security desk.
- Employees may bring a spouse, child, or visitor to the office after hours only after they have obtained written authorization of their supervisor/ manager. The written authorization to bring a guest after hours must be presented to security at the time of the visit or be on file in the security desk.
- If the employee is a supervisor or executive, he/ she will sign the visitor log indicating his/her authorization of the visitor to enter the building. (Example: Sally Smith [visitor] authorized by Jim Jones, Supervisor Court Services Unit.)
- Employees are responsible for the conduct of their escorted visitors and guests. DMV and the Commonwealth of Virginia assume no liability for employee guests in any DMV building after normal hours.

Prohibited Acts

- Employees shall not use another employee's ID or access card. Employees shall not lend nor give their ID or access card to any other person under any circumstances.
- All employees must present their ID cards to gain access to non-public areas within the DMV headquarters building. Following, tail-gating, piggy backing of another employee's access to non-public areas is prohibited.

Violations of Policy

- Violations of the building access policy, including misuse of ID/access cards, will be grounds for disciplinary actions under the Commonwealth of Virginia Standards of Employee Conduct.
- For more information regarding employee safety and security, visit myDMV and click on Employee Security or contact Kenneth Updike, Emergency Operations Manager, at (804) 367- 0066 or e-mail kenneth.updike @dmv.virginia.gov.

Department of Human Resource Management (DHRM) and State Policies and Procedures

Department of Human Resource Management Policies and Procedures Manual

Policy Number: 1.05 - Alcohol and Other Drugs

Efft. Date: 9/16/93 Updated: 11/29/06

PURPOSE

It is the Commonwealth's objective to establish and maintain a work environment free from the adverse effects of alcohol and other drugs. The effects of alcohol and other drugs in the workplace could undermine the productivity of the Commonwealth's workforce, one of Virginia's greatest assets. The adverse effects of alcohol and other drugs create a serious threat to the welfare of fellow employees and to Virginia's citizens. The Commonwealth, therefore, adopts the following policy and procedures to address alcohol and other drug problems in the public work force.

EMPLOYEES TO WHOM POLICY APPLIES

This policy applies to all Executive Branch positions whether covered or non-covered under the Virginia Personnel Act, whether full-time or part-time, or paid on a salaried or on an hourly basis. This policy also includes all teaching, research and administrative faculty, employees of the Governor's Office, the Office of the Lieutenant Governor, and the Office of the Attorney General.

Definitions

Alcohol	Any product defined as such in the Alcohol Beverage Control Act, section 4.1-100 of the Code of Virginia, as amended.
Conviction	A finding of guilty (including a plea of guilty or nolo contendere), or imposition of sentence, or both, by any judicial body charged with the responsibility of determining violations of the federal or state criminal drug laws, alcohol beverage control laws, or laws that govern driving while intoxicated.
Criminal Drug Law	Any criminal law governing the manufacture, distribution, dispensation, use, or possession of any controlled drug.
Controlled Drug	Any substance defined as such in the Drug Control Act, Chapter 34, Title 54.1 of the Code of Virginia, as amended, and whose manufacture, distribution, dispensation, use, or possession is controlled by law.
Employee	All Executive Branch employees, whether classified or non-classified, full-time or part-time, or paid on a salaried or on an hourly basis, to include all teaching, research and administrative faculty, employees of the Governor's Office, the Office of the Lieutenant Governor, and the Office of the Attorney General.
Employee Assistance Program (EAP)	A confidential assessment, referral, and short-term problem-solving service available to eligible employees and family members. Enrollment in the EAP is automatic as part of the health plan coverage. The EAP helps participants deal with problems affecting personal and work life, such as: • conflicts within the family and workplace, • personal and emotional concerns, • alcohol and substance abuse, • financial and legal problems, • elder and child care, and • career concerns and other challenges.
Management	The person(s) ultimately responsible for an employee's workplace and performance, e.g., an agency head, a secretarial branch cabinet secretary, the Governor for the Governor's office, or their official designees.

Other drug	Any substance other than alcohol that may be taken into the body and may impair mental faculties and/or physical performance.
Supervisor	The person immediately responsible for an employee's workplace and performance.
Workplace	Any state-owned or leased property, or any site where state employees are performing official duties.

EMPLOYEE RESPONSIBILITIES

Abide by policy	Employees must abide by the Commonwealth of Virginia's Policy on Alcohol and Other Drugs, and applicable disciplinary policies.
Report convictions	1. Employees must notify their supervisors of any conviction of: ○ a criminal drug law, based on conduct occurring in or outside of the workplace; or ○ an alcohol beverage control law or law that governs driving while intoxicated, based on conduct occurring in the workplace. 2. How notification given ○ Notification of a conviction must be made in writing and delivered no later than five calendar days after such conviction. 3. Effect of appeal of conviction ○ An employee's appeal of a conviction does not affect the employee's obligation to report the conviction.

VIOLATIONS

Each of the following constitutes a violation of this policy:

A.	The unlawful or unauthorized manufacture, distribution, dispensation, possession, or use of alcohol or other drugs in the workplace;
B.	Impairment in the workplace from the use of alcohol or other drugs, except from the use of drugs for legitimate medical purposes;
C.	A criminal conviction for a: 1. violation of any criminal drug law, based upon conduct occurring either on or off the workplace; or 2. violation of any alcohol beverage control law or law that governs driving while intoxicated, based upon conduct occurring in the workplace; and
D.	An employee's failure to report to his or her supervisor the employee's conviction of any offense, as required in Report Convictions.

DISCIPLINARY ACTION

For policy violation(s)	Any employee who commits any violation, as described in section IV above, shall be subject to the full range of disciplinary actions, including discharge, pursuant to applicable disciplinary policies, such as Policy 1.60, Standards of Conduct.
Severity of discipline	The severity of disciplinary action for violations of this policy shall be determined on a case-by-case basis. Mitigating circumstances that may be considered in determining the appropriate discipline include whether the employee voluntarily admits to, and seeks assistance for, an alcohol or other drug problem.

MANAGEMENT RESPONSIBILITIES

Fair application of policy	1. The Commonwealth is dedicated to assuring fair and equitable application of this policy. Therefore, management shall use and apply all aspects of this policy in an unbiased and impartial manner. 2. Any supervisor who knowingly disregards the requirements of this policy, or who is found to have deliberately misused this policy in regard to subordinates, shall be subject to disciplinary action, up to and including discharge.
Provide employees with copy of summary of policy or, upon request, copy of entire policy	1. Management must provide to every employee a copy of the Summary of the Commonwealth of Virginia's Policy on Alcohol and Other Drugs (see Attachment I), or, upon an employee's request, a copy of the entire policy. 2. Employees shall be required to sign a form indicating their receipt of either the Summary or the entire policy. This form shall be kept in the employee's personnel file.
Post policy	Management must post a copy of the entire policy in a conspicuous place or places in the workplace.
Training of agency representatives and supervisors	The Department of Human Resource Management in coordination with the Department of Employment Dispute Resolution, shall instruct agency representatives, who in turn shall instruct agency supervisors, on the implementation of this policy, including: 1. how to recognize behaviors that may indicate impairment from alcohol and/or other drug use; 2. appropriate referral techniques; and 3. resources for rehabilitation for alcohol and other drug use.
Ongoing employee education	Agencies must inform employees, on an ongoing basis, of: 1. the dangers of alcohol and/or other drug use or abuse in the workplace; 2. available counseling for alcohol and/or other drug use; 3. available rehabilitation and employee assistance programs; and 4. the penalties that may be imposed for policy violations, as set forth in the Disciplinary Section above.
Appropriate action when notified of violations	1. Within 30 calendar days of receiving notice of an employee's criminal conviction, as specified in section IV(C) above, or of any other violation of this policy, management must: ○ take appropriate disciplinary action against the employee; and/or ○ require the employee to participate satisfactorily in a rehabilitation program if a drug-related conviction is received, or recommend such a program if an alcohol-related conviction is received. An employee's satisfactory participation in a rehabilitation program shall be determined by management after: 1. the employee's presentation of adequate documentation (the agency has discretion to determine what documentation will be required); and/or 2. consultation with EAP or with any rehabilitation program, provided that the employee gives his or her consent when the consultation is to be with the rehabilitation program that treated the employee. 2. Within ten calendar days after receiving notice that an employee covered by the federal Drug Free Workplace Act has been convicted of a criminal drug

	law violation occurring in the workplace, the agency shall notify any federal contracting or granting agency.
Require contractor compliance	Management shall require contractors working on state agency workplaces to certify that they will not commit violations as described in Violations sections (A) and (B), above.

REHABILITATION PROGRAMS

Employees with problems related to the use of alcohol or other drugs are encouraged to seek counseling or other treatment.

Assistance from management	1. Management is encouraged to assist employees seeking counseling or other treatment. 2. Management should consult with the EAP before referring an eligible employee to a rehabilitation program.
Assistance from EAP	1. Eligible employees are encouraged to consult with the EAP to determine appropriate rehabilitation programs. 2. The EAP can provide information regarding health insurance coverage for rehabilitation programs. Not all programs are licensed, accredited or covered under employees' health insurance coverage.
Assistance from other agencies	Employees may contact other agencies, such as the Department of Mental Health, Mental Retardation and Substance Abuse Services, the Department of Health, the Department of Rehabilitative Services, and/or Virginia Office for Protection and Advocacy.
Leaves of absence to seek rehabilitation	1. At the discretion of management, employees may be granted leaves from work to participate in treatment programs for alcohol and/or other drug use problems. 2. Employees covered under the Virginia Personnel Act (as defined in section II (A) of Policy 2.20, Types of Employment) may use their accrued sick leave for treatment programs, as appropriate, according to Policy 4.55, Sick Leave.

AGENCY POLICIES

Agencies may promulgate supplemental alcohol and other drug policies as needed to comply with federal or state law, and as provided below.

Content of policies	1. Agencies may promulgate policies that more strictly regulate alcohol and other drugs in the workplace provided such policies are consistent with this policy. 2. The job duties of certain employees may be of such a nature that impairment from alcohol creates a great risk to the safety of others. Therefore, agencies which develop supplemental policies under this section may identify, by position Role, those positions where, because of the nature of the job duties, a conviction of an alcoholic beverage control law or law that governs driving while intoxicated that results from conduct occurring off the workplace must be reported to the agency.
Approval of policies	The Department of Human Resource Management and the Office of the Attorney General must approve supplemental agency policies before their implementation.

CONFIDENTIALITY AND MAINTENANCE OF RECORDS

DMV Supplemental Alcohol and Other Drugs Policy
(Supplement to DHRM's Policy No. 1.05: Alcohol & Other Drugs)

Revision Date: 02/22/2012

Background

The Department of Motor Vehicles' services cover a wide spectrum of motor vehicle related operations and functions, including such agency core functions as issuing driver's licenses, ID cards, vehicle titles and registrations, providing transportation safety services and enforcing and administering Virginia's motor vehicle laws. That enforcement includes denying, canceling, revoking or suspending the privilege to drive whenever a person's conduct involves the receipt of (1) a driving under the influence (DUI) conviction; (2) a refusal to submit to a blood or breathe test conviction; or (3) an administrative license suspension (ALS).

One of DMV's important missions is to advance transportation safety. DMV's goals include, among others, (1) educating the public about driving under the influence of alcohol or other drugs and the consequences of such conduct; (2) ensuring that the Commonwealth's highways are free of unsafe or irresponsible drivers; and (3) reducing traffic fatalities, especially those that are the result of people driving under the influence of alcohol and drugs.

Purpose

This supplemental policy establishes requirements for DMV employees to notify their supervisors of any conviction of a law that governs driving while under the influence of alcohol or other drugs; refusing to submit to a blood or breathe test either in or outside of the workplace; or of an administrative license suspension (ALS). In addition, it establishes disciplinary action that may be taken as a result of a conviction or a report of an ALS.

The supplemental policy is an extension of DHRM's Policy No. 1.05: Alcohol and Other Drugs. It does not replace Policy No. 1.05

Employee Responsibilities

An employee must notify his or her supervisor when the employee has been convicted of:

- a law that governs driving while under the influence of alcohol or drugs,
- a law governing refusal to submit to a blood or breathe test, based on conduct occurring either in or outside the workplace,

An employee must notify his or her supervisor when law enforcement has imposed an administrative license suspension. An ALS is imposed for a charge of DUI or refusal to submit to the Blood/Breath Test. An administrative license suspension is the act of law enforcement to suspend a driver's license immediately for a period of seven days, 60 days or until trial date dependent upon whether it is the driver's 1st, 2nd or subsequent offense.

Notification of an ALS or a conviction must be made in writing and delivered to the employee's supervisor no later than five calendar days after such conviction or ALS. An employee's appeal of a conviction or ALS does not affect the employee's obligation to report the conviction or ALS.

If the employee has filed, or plans to file, an appeal, written notice of the appeal or the intent to appeal must be provided to the employee's supervisor within five calendar days of the employee's decision to appeal.

Each employee must acknowledge receipt of this supplemental policy and must provide DMV management authorization to review the employee's driving record.

Disciplinary Action

A DMV employee who, after any appeal is exhausted, is convicted of or pleads no contest to driving under the influence of alcohol or drugs or refusal to submit to a blood or breath test, based on conduct that occurs in or outside of the workplace, will be deemed to have

committed an offense under the Standards of Conduct Policy No. 1.60. Such an offense would normally warrant a Group III written notice and discharge; however the severity of the disciplinary action will be determined on a case-by-case basis. Mitigating circumstances, if any, will be considered.

Management Responsibilities

In addition to management's responsibilities in DHRM's Alcohol and Other Drugs Policy No. 1.05, management will periodically review each employee's driving record for convictions of violations of the laws that govern driving while under the influence of alcohol or drugs and refusal to submit to a blood or breath test or an administrative license suspension. Such periodic review will take place at least once annually, normally near the end of each performance cycle.

Management should discuss all reports of a conviction or an ALS with Human Resources/Employee Relations in order to receive guidance prior to imposing disciplinary action. Discovery of an unreported conviction or ALS will be considered a violation of this policy and Standards of conduct Policy 1.60 and will normally warrant a Group III written notice and discharge. Mitigating circumstances, if any, will be considered.

www.dmvNow.com
Virginia Department of Motor Vehicles
Post Office Box 27412
Richmond, Virginia 23269-0001

ALCOHOL AND OTHER DRUGS POLICY ACKNOWLEDGEMENT

Purpose: Use this form to acknowledge receipt of and compliance with the Virginia DMV's Alcohol and Other Drugs Policy.

Instructions: Give completed form to HR Consultant or HRO, Room 124.

EMPLOYEE INFORMATION	
EMPLOYEE NAME	
EMPLOYEE TITLE	EMPLOYEE DEPARTMENT/LOCATION

POLICY

The Commonwealth of Virginia's Policy on Alcohol and other Drugs, No. 1.02, states that the following acts by employees are prohibited:

I. the unlawful or unauthorized manufacture, distribution, dispensation, possession, or use of alcohol and other drugs on the workplace;

II. the impairment on the workplace from the use of alcohol or other drugs, (except the use of drugs for legitimate medical purposes);

III. action which results in the criminal conviction for:

- a violation of any criminal drug law, based upon conduct occurring either on or off the workplace, or
- a violation of any alcoholic beverage control law, or law which governs driving while intoxicated, based upon conduct occurring on the workplace;

IV. the failure to report to their supervisors that they have been convicted of any offense, as defined in III above, within five calendar days of the conviction.

Included under this policy are all employees in Executive Branch agencies, including the Governor's Office, Office of the Lieutenant Governor, and the Office of the Attorney General.

The workplace consists of any state owned or leased property or any site where official duties are being performed by state employees.

Any employee who commits any prohibited act under this policy shall be subject to the full range of disciplinary actions, including discharge, and may be required to participate satisfactorily in an appropriate rehabilitation program.

A copy of the entire Commonwealth of Virginia's Policy on Alcohol and Other Drugs may be obtained from your agency Human Resource Office.

RECEIPT ACKNOWLEDGEMENT

Your signature below indicates your receipt of this policy summary. Your signature is intended only to acknowledge receipt, it does not imply agreement or disagreement with the policy itself. If you refuse to sign this certificate of receipt, your supervisor will be asked to initial this form indicating that a copy has been given to you.

EMPLOYEE SIGNATURE	DATE (mm/dd/yyyy)

USE OF ELECTRONIC COMMUNICATIONS AND SOCIAL MEDIA

Application: All state employees, including employees of agencies exempt from coverage of the Virginia Personnel Act.

NOTE: Agencies may also require consultants, contract personnel, or other non-employees such as volunteers or interns to abide by this policy.

PURPOSE

The purpose of this policy is to ensure the appropriate, responsible, and safe use of electronic communications and social media by employees. This policy establishes minimum standards for all state employees. Agencies may supplement this policy as necessary, as long as such supplement is consistent with this policy.

POLICY SUMMARY

This policy includes the following:

- Employee Responsibilities and Requirements
  - Business Use
  - Personal Use
  - User Requirements
  - Prohibited Activities
- Agency Responsibilities and Requirements
  - Monitor Usage
  - Communication
  - Address Violations
- Glossary and Relevant Terms
- Attachment A

AUTHORITY

This policy is issued by the Department of Human Resource Management (DHRM) pursuant to the authority provided in §2.2-1201 and §2.1-2827 of the Code of Virginia.

DHRM reserves the right to revise or eliminate this policy as necessary.

Agencies may supplement this policy to accommodate specific business needs. Supplemental policies must be consistent with the provisions of DHRM policy and must be communicated to all agency employees.

RELATED POLICIES

Policy 1.60 - Standards of Conduct

Virginia Information Technologies Agency Information Security Policy, Standards, and Guidelines

Virginia Information Technologies Agency - Information Technology Standard Use of Non-Commonwealth Computing Devices to Telework

Virginia Information Technologies Agency - Telework Resources

Office of Fleet Management Services Policies and Procedures Manual

EMPLOYEE RESPONSIBILITIES AND REQUIREMENTS

All employees must comply with this policy and any additional policies that may be adopted by the agency or institution of the Commonwealth where the user is working.

A. **Business Use**

Agency provided electronic communications tools are the property of the Commonwealth and are provided to facilitate the effective and efficient conduct of State business. Users are permitted access to the Internet and electronic communications tools to assist in the performance of their jobs. Some users may also be permitted to access and use social media to conduct agency business. Each agency or institution of the Commonwealth may adopt its own policy setting forth with specificity the work-related purposes for which such equipment and access are provided.

B. **Personal Use**

Personal use means use that is not job-related. In general, incidental and occasional personal use of the Commonwealth's electronic communications tools including the Internet is permitted as long as the personal use does not interfere with the user's productivity or work performance, does not interfere with any other employee's productivity or work performance, and does not adversely affect the efficient operation of the Commonwealth's systems and networks. Personal use of social media that refers to any aspect of the work environment should be done in a responsible and professional manner.

C. **User Requirements**

1. General Requirements

When using electronic communications tools and social media, users should:

- Follow all applicable Commonwealth policies. Users may not violate any provision of this policy, any supplemental policy adopted by agencies, or any other policy, regulation, law or guideline as set forth by local, State or Federal law (see Code of Virginia §2.2-2827) This may include but is not limited to copyright laws, trademark laws, and other legislated requirements.
- Be responsible and professional in their activities. Employees should conduct themselves in a manner that supports the mission of their agency and the performance of their duties.
- Exercise the appropriate care to protect the agency's electronic communications tools against the introduction of viruses, spyware, malware, or other harmful attacks. When using the Commonwealth's electronic communications tools, social media or Internet access, employees must:
  - Use the Internet, electronic communications tools and social media only in accordance with State and agency policy;
  - Maintain the conditions of security (including safeguarding of passwords) under which they are granted access to such media;
  - Check with the appropriate agency staff prior to downloading or accessing a file or document if the source of the file or other circumstances raises doubts about its safety.
- Be respectful of the agency/organization, other employees, customers, vendors, and others when posting and communicating information. Users should be sensitive to referring to or including others in their communications and posts and should be aware of any associated potential liabilities. Users may desire to obtain consent prior to communicating or posting information about the work place.

2. Business Use Requirements

When using electronic communications tools and social media, users should:

- Use their accurate identities and state their affiliation when using electronic communications or social media for business purposes.
- Ensure the security of sensitive or confidential information when communicating electronically or posting the information on internal or external websites including social media.
- Ensure information is accurate prior to posting on social media sites, state or agency websites, or other electronic media sites. If it is discovered that information is inaccurate after posting, users should work to quickly correct the errors.

3. Personal Use Requirements

When using electronic communications and social media, users should:

- Be clear that their communication or posting is personal and is not a communication of the agency or the Commonwealth when using electronic communications or social media for personal use, including personal use of social media outside of the work environment. For example:
  - Users should use their personal email addresses and not those related to their positions with the Commonwealth when communicating or posting information for personal use.
  - Users may use a disclaimer when posting opinions or views for personal use such as, "The views expressed on this (website, blog, social media site) are my own and do not reflect the views of my employer or of the Commonwealth of Virginia." when appropriate to ensure these views are not viewed as official Commonwealth of Virginia communications.

D. **Prohibited Activities**

Certain activities are prohibited when using the Commonwealth's Internet and electronic communications media or using social media in reference to the work environment. Employees who engage in prohibited activities may be subject to disciplinary action according to Policy 1.60, Standards of Conduct. Prohibited activities include, but are not limited to:

- Any use that is in violation of applicable local, state, and federal law.
- Accessing, uploading, downloading, transmitting, printing, posting, or storing information with sexually explicit content as prohibited by law (see Code of Virginia §2.2-2827).
- Accessing, uploading, downloading, transmitting, printing, posting, or storing fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images.
- Installing or downloading computer software, programs, or executable files contrary to the Virginia Information Technology Agency's (VITA) Information Security Policy, Standards, and Guidelines.
- Accessing, uploading, downloading, transmitting, printing, communicating, or posting access-restricted agency information, proprietary agency information, sensitive state data or records, or copyrighted materials in violation of agency or state policy.
- Using proprietary agency information, state data or records, and social media to locate agency customers for personal reasons.
- Posting information or sending electronic communications such as email using another's identity.

- Permitting a non-user to use for purposes of communicating the message of some third party individual or organization.
- Posting photos, videos, or audio recordings taken in the work environment without written consent.
- Using agency or organization logos without written consent.
- Texting, emailing, or using hand-held electronic communications devices while operating a state vehicle according to the Office of Fleet Management Services Policies and Procedures Manual.
- Any other activities designated as prohibited by the agency.

AGENCY RESPONSIBILITIES AND REQUIREMENTS

Agencies have the following responsibilities and requirements related to this policy.

A. **Monitor Usage**

No user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth's equipment and/or access. Agencies have a right to monitor any and all aspects of electronic communications and social media usage. Such monitoring may occur at any time, without notice, and without the user's permission.

In addition, except for exemptions under the Act, electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore, available for public distribution.

B. **Communication**

Agencies are responsible for ensuring employees have access to, read, understand, and acknowledge this policy and any related policies. Agencies may develop a written policy, consistent with this policy which supplements or clarifies specific issues for the agency. With regard to use of electronic communications and social media, agencies are responsible for:

- Communicating this policy and agency policy, if appropriate, to current and new users, including users transferring from other agencies.
- Retaining electronic records in accordance with the retention requirements of the Library of Virginia.
- Requiring and retaining acknowledgement statements, signed by each user, acknowledging receipt of a copy of this policy and agency policy, if appropriate. A sample is attached (Attachment A) that agencies may use, or they may include the acknowledgement statement with other such statements obtained when employees are hired.

NOTE: Agencies also may develop procedures by which a user must actively

acknowledge reading the policy before access to electronic communications and social media will be granted.

C. **Address Violations**

Violations of this policy must be addressed under Policy 1.60, Standards of Conduct, or appropriate disciplinary policy or procedures for employees not covered by the Virginia Personnel Act. The appropriate level of disciplinary action will be determined on a case-by-case basis by the agency head or designee, with sanctions up to or including termination depending on the severity of the offense, consistent with Policy 1.60 or the appropriate applicable policy.

GLOSSARY AND RELEVANT TERMS

Blog
A contraction of "web log" that is a website or part of a website with commentary, descriptions of events, or journal type entries usually with an ability for readers to reply and post comments.

Computer Network
Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Crowdsourcing
An open call, usually through an Internet based resource, to an undefined community of people to obtain and use ideas, content, or solutions to business needs.

Electronic Communications Tools
Tools used as a means of sending and receiving messages or information electronically through connected electronic systems or the Internet. Tools may include networked computers, email, voicemail, cell phones, smart phones, any other similar system, and new technologies as they are developed.

Internet
An international network of independent computer systems. The World Wide Web is one of the most recognized means of using the Internet.

Microblog
A form of a blog in which frequent, short updates are posted about specific activities (e.g., Twitter).

Photo Sharing
The online publishing of photographs with the ability to transfer and share the photos with others.

Podcast
Digital media file that can be downloaded for playback to computers and personal digital devices.

Social Media
Form of online communication or publication that allows for multi-directional interaction. Social media includes, blogs, wikis, podcasts, social networks, photograph and video hosting websites, crowdsourcing, and new technologies as they evolve.

Social Networking
Interacting with a group of people with common interests in a virtual environment.

Users
All employees of the Commonwealth who use the Commonwealth's Internet access and/or electronic communications media or external electronic communications media to communicate about the Commonwealth's activities.

NOTE: Agencies may also require consultants, contract personnel, or other non-employees such as volunteers or interns to abide by this policy.

Video Sharing
The online publishing of videos with the ability to transfer and share them with others.

Wikis
A collaborative website that allows users to edit materials and information posted and to create collaborative solutions for identified topics.

ATTACHMENT A

Use of Electronic Communications and Social Media

CERTIFICATE OF RECEIPT

I have been given a copy of Department of Human Resource Management Policy 1.75, "Use of Electronic Communications and Social Media" and I understand that it is my responsibility to read and abide by this policy, even if I do not agree with it. If I have any questions about the policy, I understand that I need to ask my supervisor or the agency/institution Human Resource Officer for clarification.

I understand that no user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth's equipment and/or access. Agencies have a right to monitor any and all aspects of electronic communications and social media usage. Such monitoring may occur at any time, without notice, and without the user's permission.

In addition, except for exemptions under the Act, electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore, available for public distribution.

If I refuse to sign this certificate of receipt, my supervisor will review this statement with me and will be asked to initial this form indicating that a copy has been given to me and that this statement has been read to me.

Employee's Name: _____

Employee Number: _____

Signature: _____

Date: _____

DMV Supplemental Policy — Social Media

Revision Date: 03/2012

Purpose:

This policy is a supplement to the Department of Human Resource Management Policy on Use of Electronic Communications and Social Media Policy (Policy 1.75). The purpose of this policy is to ensure the appropriate, responsible, and safe use of electronic communications and social media by employees. This policy establishes minimum standards, and provides employees with general guidelines to protect the Department of Motor Vehicles and its employees from unauthorized disclosure of confidential information and inappropriate exposure due to personal social media.

Note: In regards to the use of state electronic equipment and communication for business purposes, DMV employees must adhere to: the Commonwealth of Virginia Policy on Use of Electronic Communications and Social Media Policy (Policy 1.75) and the Virginia Information Technologies Agency Information Security Policy, Standards, and Guidelines; the DMV IT Security Policy; and the DMV Acceptable Use Policy.

Definitions

Term	Definitions
Apps	Apps are simply an application that performs a specific function on your computer, tablet or handheld device. Apps run the gamut from Web browsers and games to specialized programs like digital recorders, online chat or music players.
Blog	A blend of "web" and "log" that is a journal published on a website consisting of periodic entries and usually provides the ability to reply and post comments.
Electronic Communications Tools	Tools used as a means of sending and receiving messages or information electronically through connected electronic systems or the Internet. Tools may include networked computers, email, voicemail, cell phones, smart phones, any other similar system, and new technologies as they are developed.
Photo Sharing	The online publishing of photographs with the ability to transfer and share the photos with others.
Smart Phone	Smart phone is a handheld device capable of advanced tasks beyond those of a standard mobile phone including iPhone, Droid, and Blackberry. Capabilities including email, chat, taking photos or video or hundreds of other tasks including downloading and accessing apps.
Social Networking	Interacting with a group of people with common interests in a virtual environment.
Stickiness	Stickiness is having viewers return to the social media outlets for new content and material. Ideally, viewers will continue to return to the pages for information, prizes, and contests instead of “liking” or following the page once. Message penetration works best when viewers are engaged and actively participating.
Video Sharing	Uploading videos to a website providing the ability to transfer and share with others.

Applies To:

This policy applies to all employees working at DMV, full-time and part-time classified employees, and wage (P14) employees. This policy also applies to contractors/ consultants while working at DMV.

General Provisions:

DMV respects the rights of its employees, during their personal time and using their personal equipment, to use blogs and other social media as a means of self-expression and communication; and does not discriminate against employees who use these media for personal interests, affiliations or other lawful purposes. DMV employees may not use DMV secured computers (COV) to access social media accounts without prior approval from the Information Technology Security Officer.

Employees' use of and conduct within social media websites must not violate the DMV Employee Code of Conduct, DMV policies, Commonwealth of Virginia Standards of Conduct, or the Commonwealth of Virginia Workplace Harassment Policy. Employees are expected to maintain a clear line between "you" as the individual and "you" as the employee. The following provisions are provided to give employees a "best practice" approach to using social media for personal and/or non-business use.

Standard Guidelines

- Social networking applications may only be used during work hours by employees directly assigned and approved to access them as part of their work at DMV. Personal use of social media should only be done on employees' own time and equipment.
- Employees should not use social media in any manner that would be considered to be not in compliance with any of the following guidelines:

  Be dedicated to the PEAK (People, Ethics, Accuracy and Knowledge),

  Adhere to all policies and procedures of the Department of Motor Vehicles,

  Safeguard and secure all information which is personal, confidential, and/or protected by state or federal law and/or regulation,

  Guard against conflict of interest and the appearance of impropriety,

  Oppose all forms of discrimination and harassment,

  Act with honesty and integrity at all times,

  Treat everyone fairly, impartially, consistently and without partisanship,

  Demonstrate respect for the agency and toward agency coworkers, supervisors, managers and customers,

  Support efforts that ensure a safe and healthy work environment

  Resolve work-related issues and disputes in a professional manner and through established business processes,

  Comply with the letter and spirit of all state agency policies and procedures and Commonwealth of Virginia laws and regulations, or

  Conduct oneself at all times in a manner that supports the mission of the agency.

- Employees should not use social media to harass, bully, intimidate, threaten, criticize, or discriminate against any other employee, or anyone associated with or doing business with DMV, or to engage in any form of retaliation directed against another employee or anyone associated with or doing business with DMV who has complained about harassment or participated in any investigation concerning harassment.
- Employees should not post on blogs or other social media sites unauthorized photographs of other employees, customers, vendors or suppliers while engaged in agency business or agency sponsored events.
- Employees should refrain from posting information which is not subject to public disclosure about the agency or its projects/ programs on social media sites.
- DMV social websites, pages or accounts maintained by DMV are intended to be the "official voice" of the agency:

  Employees should not add to or edit the content of such material unless they are assigned to do as part of their job responsibilities.

  Employees should not speak for or claim to speak for DMV on such application unless authorized to do so.

- Employees using social media may want to post a "disclaimer" along with any content that is related directly or indirectly to DMV or their job responsibilities and experiences in order to make it clear that the information posted is not meant in any way to speak for the agency or its

policies/ practices. A sample of such a disclaimer is: "*The opinions and information expressed in this post are my personal thoughts and opinions. I am in no way intending to represent the Virginia Department of Motor Vehicles (VADMV) or the Commonwealth of Virginia when sharing this information.*"

Prohibited Activities per State Policy

(Excerpts from Policy 1.75, Use of Electronic Communications and Social Media)

Certain activities are prohibited by State policy when using the Commonwealth's Internet and electronic communications media or using social media in reference to the work environment. These are:

- Any use that is in violation of applicable local, state, and federal law.
- Accessing, uploading, downloading, transmitting, printing, posting, or storing information with sexually explicit content as prohibited by law (see Code of Virginia §2.2-2827).
- Accessing, uploading, downloading, transmitting, printing, posting, or storing fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images.
- Installing or downloading computer software, programs, or executable files contrary to the Virginia Information Technology Agency's (VITA) Information Security Policy, Standards, and Guidelines.
- Accessing, uploading, downloading, transmitting, printing, communicating, or posting access-restricted agency information, proprietary agency information, sensitive state data or records, or copyrighted materials in violation of agency or state policy.
- Using proprietary agency information, state data or records, to locate agency customers for personal reasons.
- Posting information or sending electronic communications such as email using another's identity.
- Permitting a non-user to use for purposes of communicating the message of some third party individual or organization.
- Posting photos, videos, or audio recordings taken in the work environment without written consent.
- Using agency or organization logos without written consent.
- Texting, emailing, or using hand-held electronic communications devices while operating a state vehicle, according to the Office of Fleet Management Services Policies and Procedures Manual.

Violations

Violations of this policy will be addressed under Policy 1.60, Standards of Conduct Policy. Situations that are brought into the workplace as a result of matters arising from social media will become an employee relations matter and will be addressed using the Standards of Conduct.

Note: Separate from a violation of the Agency's Social Media Policy and Policy 1.75, parties involved may also be subject to personal liability and criminal prosecution if a state and/or federal law has been violated. In such case, personal liability is on an individual basis and does not necessarily impact or influence how a situation is addressed in the workplace using the Standards of Conduct.

Related Policies

- Use of Internet and Electronic Communication Systems (Policy 1.75)
- DMV IT Security Policy
- Virginia Information Technologies Agency (VITA) - Information Security Policy, Standards, and Guidelines
- VITA - Information Technology Standard Use of Non-Commonwealth Computing Devices to Telework
- VITA - Telework Resources
- Intellectual Property and Copyrightable Material
- Internet and E-mail Usage
- Acceptable Use Policy
- Backup and Recovery Operations
- LAN Usage Policy
- Remote Access to DMV Systems
- Virtual Private Network
- Office of Fleet Management Services Policies and Procedures Manual
- Standards of Conduct (Policy 1.60)

Questions about this policy should be referred to the Human Resources Office.

Department of Human Resource Management
Policies and Procedures Manual

Policy Number: 1.80 - Workplace Violence

Efft. Date: 5/01/02

Application: Full-time and part-time classified, "at will" and hourly employees.

PURPOSE

To establish a procedure that prohibits violence in the workplace.

DEFINITIONS

Third Parties	Individuals who are not state employees, such as relatives, acquaintances, or strangers.
Workplace	Any location, either permanent or temporary, where an employee performs any work-related duty. This includes, but is not limited to, the buildings and the surrounding perimeters, including the parking lots, field locations, alternate work locations, and travel to and from work assignments.
Workplace Violence	Any physical assault, threatening behavior or verbal abuse occurring in the workplace by employees or third parties. It includes, but is not limited to, beating, stabbing, suicide, shooting, rape, attempted suicide, psychological trauma such as threats, obscene phone calls, an intimidating presence, and harassment of any nature such as stalking, shouting or swearing.

PROHIBITED ACTIONS

Prohibited conduct includes, but is not limited to:

- injuring another person physically;
- engaging in behavior that creates a reasonable fear of injury to another person;
- engaging in behavior that subjects another individual to extreme emotional distress;
- possessing, brandishing, or using a weapon that is not required by the individual's position while on state premises or engaged in state business;
- intentionally damaging property;
- threatening to injure an individual or to damage property;
- committing injurious acts motivated by, or related to, domestic violence or sexual harassment; and
- retaliating against any employee who, in good faith, reports a violation of this policy.

Note: Employees may be authorized by their agencies to possess weapons in the workplace if they are required as a part of employees' job duties with the Commonwealth.

POLICY VIOLATIONS

Employees violating this policy will be subject to disciplinary action under Policy 1.60, Standards of Conduct, up to and including termination, based on the situation.

Violent acts of employees occurring outside the workplace also may be grounds for disciplinary action, up to and including dismissal. In these situations, the agency must demonstrate in writing that the violent conduct committed has an adverse impact on the employee's ability to perform the assigned duties and responsibilities or that it undermines the effectiveness of the agency's activities.

AGENCY RESPONSIBILITIES

Agency Procedures	Each agency is expected to create and maintain a workplace designed to prevent or deter workplace violence through the development of agency policies and procedures that articulate how this policy will be implemented in their agency. At a minimum, each agency must: • communicate a policy statement prohibiting workplace violence, and agency procedures for addressing such situations; • designate a coordinator to be responsible for the overall implementation of a workplace violence prevention program; • assess the agency's vulnerability for workplace violence (threat assessment); • develop and implement a plan to address and prevent workplace violence (crisis management plan); • establish a mechanism for employees to report threats that protects the safety and anonymity of anyone who comes forward with concerns about a threat or act of violence; • protect victims of workplace violence; • provide for the training of supervisors and managers in recognizing conditions that might contribute to workplace violence, and to properly address and respond to these situations; • provide training to employees about recognizing and responding to potentially violent or violent situations in the workplace; • establish relationships with appropriate supportive services that may need to be contacted in response to workplace violence; and • provide information to employees about resources and services available to them in response to workplace violence, and the potential for domestic violence to enter the workplace.

DHRM RESPONSIBILITIES

The Department of Human Resource Management will:

- provide periodic training for agency coordinators in workplace violence prevention and management,
- provide periodic training for agency supervisors and employees on workplace violence, and
- assist agencies with development of their workplace violence programs and plans.

AUTHORITY

The Department of Human Resource Management issues this policy pursuant to the authority provided in Chapter 10, Title 2.2 of the Code of Virginia.

INTERPRETATION

The Director of the Department of Human Resource Management is responsible for official interpretation of this policy, in accordance with § 2.2-1201(13) of the Code of Virginia.

Questions regarding the application of this policy should be directed to the Department of Human Resource Management's Office of Compensation and Policy or the Office of Equal Employment Services.

The Department of Human Resource Management reserves the right to revise or eliminate this policy.

RELATED POLICIES

- Policy 1.60, Standards of Conduct
- Policy 2.30, Workplace Harassment

WORKPLACE HARASSMENT

Application: Full-time and part-time classified, "at will" and hourly employees.

POLICY

It is the policy of the Commonwealth to provide its employees with a workplace free from harassment and/or retaliation against employees who either complain of harassment or aide in the investigation of such a complaint.

PURPOSE

To educate employees in the recognition and prevention of illegal workplace harassment and to provide an effective means of eliminating such harassment from the workplace.

AUTHORITY

The Director of the Department of Human Resource Management (DHRM) issues this policy and is responsible for the official interpretation of this policy pursuant to the authority provided in § 2.2-1201 of the Code of Virginia. DHRM reserves the right to revise or eliminate this policy as necessary.

Agencies may supplement this policy to accommodate specific business needs. Supplemental policies must be consistent with the provisions of DHRM policy and must be communicated to all agency employees.

RELATED POLICIES

Policy 1.60, Standards of Conduct
Policy 1.80, Workplace Violence
Policy 2.05, Equal Employment Opportunity

ADMINISTRATIVE PROCEDURES

WORKPLACE HARASSMENT

A. Prohibited Conduct

1. Harassment

The Commonwealth strictly forbids harassment of any employee, applicant for employment, vendor, contractor or volunteer on the basis of an individual's race, sex, color, national origin, religion, age, veteran status, political affiliation or disability.

2. Retaliation

The Commonwealth will not tolerate any form of retaliation directed against an employee or third party who either complains about harassment or who participates in any investigation concerning harassment.

B. Harassment Complaint Procedure

Employees and third parties should report incidents of workplace harassment as soon as possible after the incident occurs.

Employees and applicants for employment seeking to remedy workplace harassment may file a complaint with the agency human resource director, the agency head, their supervisor(s), or any individual(s) designated by the agency to receive such reports. **Under no circumstances shall the individual alleging harassment be required to file a complaint with the alleged harasser.**

1. State Complaint Procedure

The employee or applicant may follow the Commonwealth Employees' Discrimination Complaint Procedure, which is administered by the Office of Equal Employment Services within the Department of Human Resource Management.

2. Grievance Procedure

Eligible employees also may use the State Employee Grievance Procedure, which is administered by the Department of Employment Dispute Resolution, to address harassment.

3. Federal Complaint Process

Employees (and applicants for Commonwealth employment) also may file a complaint with the federal Equal Employment Opportunity Commission

4. Assurance Against Retaliation

Employees and third parties who make complaints of workplace harassment or provide information related to such complaints will be protected against retaliation. If retaliation occurs, the complainant(s) should report the retaliation through the harassment complaint procedure

C. Policy Violations

1. Engaging In Harassment

Any employee who engages in conduct determined to be harassment or encourages such conduct by others shall be subject to corrective action, up to and including termination, under Policy 1.60, Standards of Conduct.

2. Allowing Harassment to Continue

Managers and/or supervisors who allow workplace harassment to continue or fail to take appropriate corrective action upon becoming aware of the harassment may be considered parties to the offense, even though they may not have engaged in the harassment behavior.

3. Failure to Respond

Managers and/or supervisors who allow workplace harassment to continue or who fail to take appropriate action should be subject to disciplinary action, including demotion or termination, under Policy 1.60, Standards of Conduct.,.

D. Agency Responsibilities

Agencies must communicate this policy to employees and third parties.
Communication must include:

- educating employees about the types of behavior that can be considered workplace harassment, and
- explaining procedures established for filing workplace harassment complaints.

Agency managers and supervisors are required to:

- stop any workplace harassment of which they are aware, whether or not a complaint has been made;
- express strong disapproval of all forms of workplace harassment;
- intervene when they observe any acts that may be considered workplace harassment;
- take immediate action to prevent retaliation towards the complaining party or any participant in an investigation; and
- take immediate action to eliminate any hostile work environment where there has been a complaint of workplace harassment.

GLOSSARY

Retaliation
Overt or covert acts of reprisal, interference, restraint, penalty, discrimination, intimidation, or harassment against an individual or group exercising rights under this policy.

Sexual Harassment
Any unwelcome sexual advance, request for sexual favors, or verbal, written or physical conduct of a sexual nature by a manager, supervisor, co-workers or non-employee (third party).

- **Quid pro quo –** A form of sexual harassment when a manager/supervisor or a person of authority gives or withholds a work-related benefit in exchange for sexual favors. Typically, the harasser requires sexual favors from the victim, either rewarding or punishing the victim in some way.
- **Hostile environment** – A form of sexual harassment when a victim is subjected to unwelcome and severe or pervasive repeated sexual comments, innuendoes, touching, or other conduct of a sexual nature which creates an intimidating or offensive place for employees to work.

Third Parties
Individuals who are not state employees, but who have business interactions with state employees. Such individuals include, but are not limited to:

- customers, including applicants for state employment or services;
- vendors;
- contractors; or
- volunteers.

Workplace Harassment
Any unwelcome verbal, written or physical conduct that either denigrates or shows hostility or aversion towards a person on the basis of race, sex, color, national origin, religion, age, veteran status, political affiliation, or disability, that: (1) has the purpose or effect of creating an intimidating, hostile or offensive work environment; (2) has the purpose or effect of unreasonably interfering with an employee's work performance; or (3) affects an employee's employment opportunities or compensation.

Grievance Procedure

The grievance procedure is a process through which a Virginia state government employee can bring workplace concerns to upper levels of management. This process is more formal than mediation and requires that rules be followed strictly. The Grievance Procedure Manual lists the rules that must be followed. Failure to follow these strict procedures will forfeit your right to this process.

A grievance can have up to four phases: (1) the management resolution steps; (2) qualification for hearing; (3) hearing; and (4) review of the hearing decision. Not all grievances are qualified for hearing. For example, under the grievance statues, grievances that relate solely to layoffs, transfers, assignments, or the content of personnel policies, cannot proceed on to a hearing. On the other hand, some issues are automatically qualified for hearing, such as formal discipline or dismissal for unsatisfactory performance. Attorneys serving as Administrative Hearing Officers conduct hearings in qualifying grievances.

Even if your concern is about an issue that cannot be qualified for hearing, it is important to note that many grievances result in resolution during the management steps, without a grievance hearing. For more information regarding the grievance process contact the EDR AdviceLine at 1-888-23-ADVICE (1-888-232-3842).

Probationary and P-14 (hourly) employees are not eligible for the grievance procedures.

Required DMV Online Training

Required DMV Online Training Courses

DMV's required online training courses are offered through the DMV Knowledge Center.

DMV Knowledge Center Access

Go to the DMV intranet home page, click the **All Training Events** link under the agency calendar and click the LOGIN button. Or, go directly to the web address: https://covkc.virginia.gov/dmv

LOGIN ID: Use the last seven digits of your Employee ID number located on your Employee ID badge.

PASSWORD: Click the **Forgot Password** link on the DMV Knowledge Center login page to receive your temporary password at your DMV email address. If your DMV email address is not yet active, contact the DMV Knowledge Center Help Desk: (804) 367-1816 or dmvkcadmin@dmv.virginia.gov

At the blue menu bar, go to the **Learning Center** and select **Bundles** in the drop-down box. Enter **"DMV required"** in the search text box and click **Search**. Click this title: **DMV Required Courses for All Employees**. It contains the following online courses:

DMV IT: Acceptable Use Policy (30 minutes)

Completion: **First five days** of employment
Provides new employees with an overview of the acceptable use of the Commonwealth of Virginia's information technology resources.

DMV IT: Security Awareness (30 minutes)

Completion: **First 30 days** of employment
Instructs new employees how to be safe and secure in their use of Commonwealth of Virginia Information Technology resources.

DMV HR: Employee Code of Conduct (30 minutes)

Completion: **First 90 days** of employment
Outlines the standards of behavior all employees are expected and required to follow.

CoV Terrorism Security Awareness (30 minutes)

Completion: **First 90 days** of employment
Prepares new employees to recognize, react and report to potential terrorist incidents.

DMV HR: Social Media Policy (30 minutes)

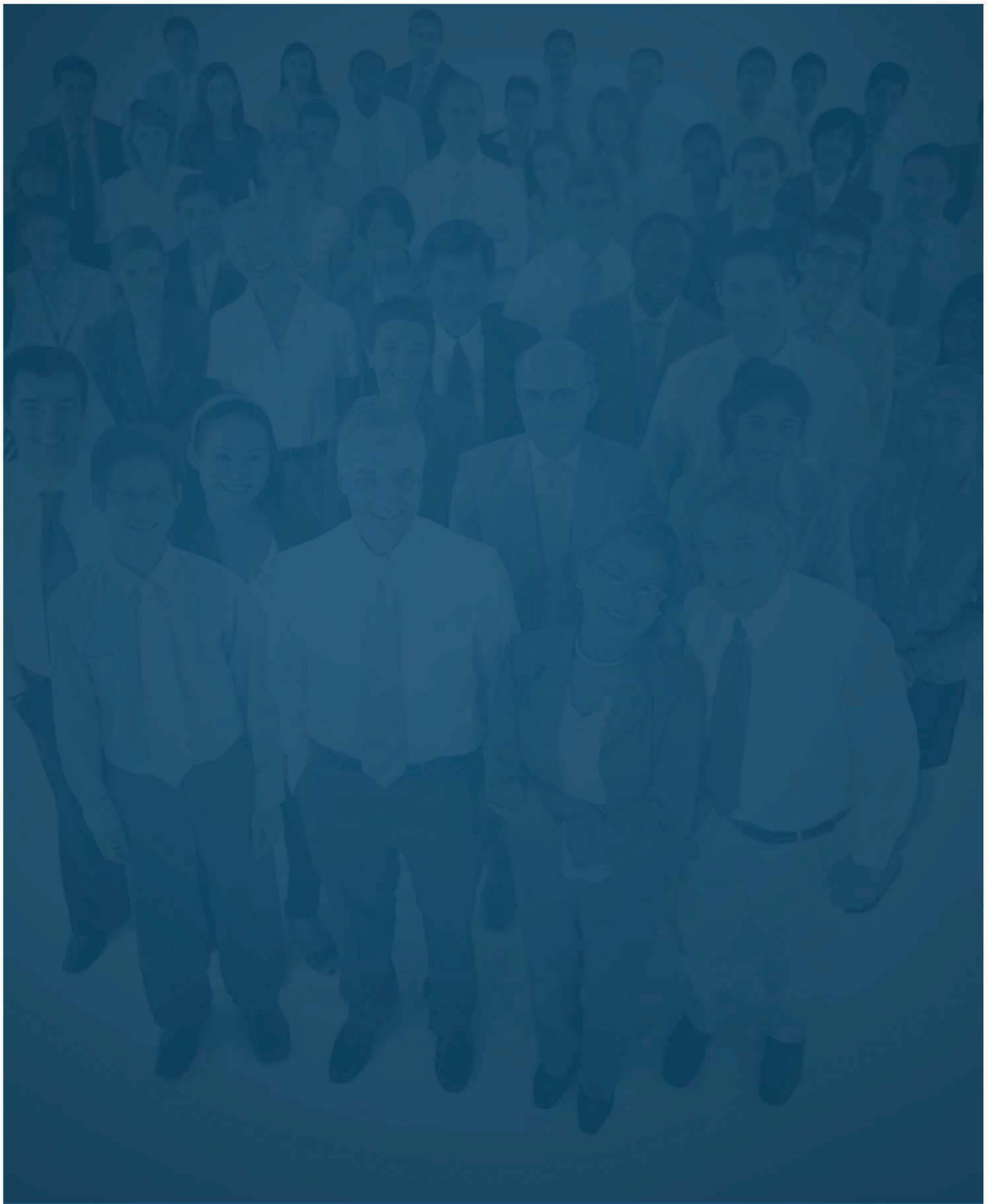
Completion: **First 90 days** of employment
Prepares new DMV employees to interface with social media in an appropriate and professional manner.

DHRM-HR Policy: Alcohol and Other Drugs (30 minutes)

Completion: **First 90 days** of employment
Informs new employees of responsibilities, reporting procedures and available resources.

DHRM-HR Policy: Preventing Workplace Violence (30 minutes)

Completion: **First 90 days** of employment
Informs new employees of responsibilities, reporting procedures and available resources.



www.dmvNow.com

DMV 220B Rev 2-2017