Virginia Department of Accounts

Acceptable Use Policy And Agreement

:

Publication Version Control

Publication Version Control: It is the user's responsibility to ensure they have the latest version of this publication. Questions should be directed to the Virginia Department of Accounts (DOA) Information Security Officer (ISO) within the Information Technology and Systems Office. The DOA ISO will issue an Agency-wide broadcast of any/all revisions and provide an email announcement to Agency Directors as well as other parties the DOA ISO considers to be interested in the revisions.

This chart contains a history of this publication's revisions.

Version	Date	Comments
Original	April 1, 2014	Updated to reflect SEC501-08 standards
1.0	April 1, 2015	Updated to reflect SEC501-09 standards, replace D. Salked with P. Tauer, CTO

Review Process: The DOA ISO and staff of the Information Technology and Systems Office contributed to the review of this publication. All comments were carefully evaluated, and individuals that provided comments were notified of the actions taken.

Information Security Policy Reviews and Approvals

Review Date	Signature	Approval Date	Signature
04/15/14	Frank J. Pitera – Information Security Officer	04/15/14	Frank J. Pitera – Information Security Officer
04/15/15	Dick Salkeld – Director Systems Development	04/15/15	Dick Salkeld – Director Systems Development
08/15/17	Frank J. Pitera – Information Security Officer	08/15/17	Pam Tauer – Chief Technology Officer

Table of Contents

1. Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Department of Accounts (DOA) in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

State Law (Article 7.1 of Title 18.2 of the Code of Virginia) classifies damage to computer hardware or software (18.2152.4), invasion of privacy (18.2152.5), or theft of computer services (18.2152.6) of computer systems as (misdemeanor) crimes. Computer fraud (18.2152.3) and use of a computer as an instrument of forgery (18.2152.14) can be felonies. DOA's internal procedures for enforcement of its policy are independent of possible prosecution under the law.

DOA provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This agreement requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2. Scope

All employees, contractors, consultants, temporary and other workers at DOA, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by DOA, or to devices that connect to a DOA network or reside at a DOA site.

Information Security must approve exceptions to this policy in advance through DOA's Exception Policy and Procedures.

3. Policy Statement

3.1. General Requirements

3.1.1. All users of DOA IT resources must adhere to Virginia Department of Human Resource Management Policy 1.75 – Use of Internet and Electronic Communication Systems.

3.1.2. You are responsible for exercising good judgment regarding appropriate use of DOA resources in accordance with DOA's policies, standards, and guidelines to ensure the protection of Personal Identifiable Information (PII). DOA resources may not be used for any unlawful or prohibited purpose.

3.1.3. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the DOA network may be

disconnected.

3.1.4. Users should report any violation of the policy by another individual and any information relating to a security flaw or compromise to the DOA Information Security Officer.

3.2. System Accounts

3.2.1. You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.2.2. You must maintain system-level and user-level passwords in accordance with the Password Policy.

3.2.3. You must ensure through legal or technical means that proprietary information remains within the control of DOA at all times. Conducting DOA business that results in the storage of proprietary information on personal or non-DOA controlled environments, including devices maintained by a third party with whom DOA does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by DOA, or its customer and partners, for company business.

3.3. Computing Assets

3.3.1. You are responsible for ensuring the protection of assigned DOA assets at all times. Laptops left at DOA overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of DOA assets to the Information Security Officer or designate.

3.3.2. Devices that connect to the DOA network must comply with the DOA Logical Access Policy.

3.3.3. Do not interfere with corporate device management or security system software, including, but not limited to, antivirus and COV Account Management..

3.4. Network Use

You are responsible for the security and appropriate use of DOA network resources under your control. Using DOA resources for the following is strictly prohibited:

3.4.1. Installing or using proprietary encryption hardware/software on DOA systems.

3.4.2. Tampering with security controls configured on DOA assets.

3.4.3. Installing personal software on DOA assets.

3.4.4. Causing a security breach to either DOA or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

3.4.5. Causing a disruption of service to either DOA or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.4.6. Adding hardware to, removing hardware from, or modifying hardware on a DOA system.

3.4.7. Connecting non-DOA-owned devices to a DOA IT system or network, such as personal computers, laptops or hand held devices, except in accordance with the current version of the Use of non-Commonwealth Computing Devices to Telework Standard (COV ITRM Standard SEC511).

3.4.8. Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

3.4.9. Use of the Internet or DOA's network that violates DOA policies, or federal, state and/or local laws.

3.4.10. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and key loggers.

3.4.11. Port scanning or security scanning on a production network unless authorized in advance by Information Security.

3.5. Electronic Communications

The following are strictly prohibited:

3.5.1. Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates DOA's policies against harassment or the safeguarding of confidential or proprietary information.

3.5.2. Sending spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

3.5.3. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

3.5.4. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3.5.5. Use of a DOA e-mail or IP address to engage in conduct that violates DOA policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a DOA e-mail or IP address represents DOA to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

3.6. Monitoring

3.6.1. Monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with DOA.

1. DOA employees should immediately report violations of information security policies to the Information Security Officer or designee.

2. If the accused is an employee, the Agency Head, ISO or designee will collect the facts of the case and identify the offender. If, in the opinion of the Agency Head, the alleged violation is of a serious nature, the Agency Head will determine the appropriate disciplinary action. Disciplinary actions may include but are not limited to:

   a. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months.
   b. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the cost associated with determining the case facts.
   c. Disciplinary action for classified staff in accordance with the guidelines established in the State Standards of Conduct Policy.

3. The Agency Head or designee will report any violations of state and federal law to the appropriate authorities.

4. All formal disciplinary actions taken under this policy are subject to the Commonwealth’s personnel guidelines and the accused may pursue findings through the appropriate grievance procedure.

5. Electronic Signature and Acceptance

The Authorized User agrees that acceptance of this Policy and Agreement by electronic means constitutes and understanding that the user may have access to information that may be of a confidential and/or sensitive nature. The user understands and is aware that it is the user's responsibility to help DOA maintain and protect the confidentiality of any information that the user has access to. Additionally, the user agrees to abide by all applicable federal, state, and local laws, as well as agency policies regarding the handling and dissemination of confidential and/or sensitive information.