



VIRGINIA DEPARTMENT OF
SOCIAL SERVICES

INFORMATION RESOURCE ACCEPTABLE USE POLICY

Prepared By:
Information Security and Risk Management



Date Document Prepared:
September 2016

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 Social Services (VDSS) Chief Information Security Officer (CISO) within the Information Security and Risk Management (ISRM) Office. The VDSS CISO will issue an agency-wide Broadcast and post the revised publication version on the Services.Programs.Answers.Resources.Knowledge (SPARK) Intranet, and provide an email announcement to division/directorate/office/district/regions and Local Departments of Social Services (LDSS) Security Officers as well as other parties the VDSS CISO considers being interested in the change.

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

Version	Date	Comments
Original	June 10, 2011	
Revision 1	September 30, 2014	Significant re-write and update to include account use, network access, overuse, copyright infringement, remote access, protecting electronic devices, protecting data, peer-to-peer file sharing, bandwidth use, incidental use, use for illegal activities, personal storage media, software installation, and IT equipment and software purchases.
Revision 2	June 2015	Email clarification. Flash drives.
Revision 3	March 2016	Policy name change. Removed redundant account use section.
Revision 4	September 2016	Removed (Employee Work Profile) EWP and replaced with employee's job description and responsibilities. Updated Code of Virginia hyperlinks.

Review Process: The VDSS CISO and staff of the ISRM Office contributed to the review of this publication. All comments were carefully evaluated, and individuals that provided comments were notified of the actions taken.

PREFACE

Subject

The VDSS Information Resource Acceptable Use Policy

Effective Date: *March 4, 2016*

Authority

The policies described in this document are based on requirements found in the following codes, policies, regulations, laws, standards, and guidelines:

Code of Virginia, [§ 2.2-2005, et. seq.](#)

Powers and duties of the Chief Information Officer “CIO”
Virginia Information Technologies Agency, “VITA”

Code of Virginia, [§ 2.2-2009, et. seq.](#)

Additional duties of the CIO relating to security of
government databases

Code of Virginia, [§ 2.2-2827](#)

Restrictions on state employee access to information
infrastructure

Code of Virginia, [§2.2, Chapter 12](#)

Department Human Resource Management, DHRM

Other References

[DHRM Policy No. 1.75, Use of Electronic Communications
and Social Media](#) (.pdf)

[VDSS Information Security Policy and Program Guide](#) (.pdf)

Purpose

The purpose of this policy is to create a prescriptive set of processes and procedures; aligned with applicable Commonwealth of Virginia (COV) Information Technology (IT) security policy and standards, to ensure the Virginia Department of Social Services (VDSS) develops, disseminates, and updates the **VDSS Information Resource Acceptable Use Policy**. This policy and procedure establishes the minimum requirements for the **VDSS Information Resource Acceptable Use Policy**.

Scope

This policy applies to:

All *individuals* (VDSS employees, LDSS employees, contractors, vendors, volunteers, student interns, work experience personnel, and other persons and organizations including the Virginia Department of Medical Assistance Services’ (DMAS)) who have a need to use VDSS- sponsored Internet, email, other electronic communications VDSS-related information or information processing systems.

All information and information processing systems associated with other organizations which VDSS uses, including but not limited to the Social Security Administration (SSA), the Virginia Department of Taxation (TAX), the Internal Revenue Service (IRS), the Department of Motor Vehicles (DMV), and the Virginia Employment Commission (VEC).

Table of Contents

A.	General Statements	1
B.	Internet Use	1
C.	Network Access.....	2
D.	Unacceptable Use	3
E.	Overuse	4
F.	Copyright Infringement.....	4
G.	Remote Access	5
H.	Email Use.....	5
I.	Protecting Electronic Devices	6
J.	Protecting Data	7
K.	Peer-To-Peer File (P2P) Sharing	7
L.	Bandwidth Use	7
M.	Incidental Use	7
N.	Use for Illegal Activities.....	8
O.	Personal Storage Media	8
P.	Flash Drives	9
Q.	Software Installation.....	9
R.	Information Technology (IT) Equipment and Software Purchases	10
S.	Acceptance and Violations of Policy	10

A. General Statements

1. VDSS system users should have no expectation of privacy in regard to any message, file, email, image or data created, sent, viewed, retrieved, or received when using VDSS or Commonwealth of Virginia (COV)-provided equipment or access. VDSS reserves the right to monitor computer networks, electronic communication systems, the Internet, and VDSS systems at any time, without notice and without the user's permission.
2. All electronic records may be subject to the Freedom of Information Act (FOIA) and available for public distribution.
3. All individuals and organizations that use VDSS-sponsored Internet, email, other electronic communications, and VDSS systems will abide by COV and VDSS' policies and procedures.
4. Users should avoid routine personal communications on electronic communication systems provided by the COV to include computer systems, the Internet, email, office phones, mobile cell phone devices, social media web sites, and voice mail provided for official business.
5. Users are expected to be responsible and professional when using COV-sponsored electronic communication services whether for personal or professional purposes.
6. Directors may augment this policy with more restrictions. If so, they should first submit their planned restrictions to the VDSS Chief Information Security Officer (CISO) for review. This augmentation should clearly communicate to employees, in written form, their expectations on the allowable use of Internet, email, and other electronic communication to ensure a clear understanding of unacceptable use if it is more restrictive than this policy.

Note: This policy does not attempt to define all acceptable or unacceptable personal use. The information included in this policy is provided as a guideline. If the employee is unclear about acceptable personal use, he/she should seek the advice of his/her supervisor or Division Director.

B. Internet Use

1. Acceptable use of the Internet consists of activities necessary to support the purpose, goals, and mission of VDSS and each user's authorized job functions as expressed in the employee's job description and responsibilities.
2. VDSS has implemented the following monitoring capabilities:
 - a. Log Internet access;



- b. Monitor the Internet access and usage by individuals; and
 - c. Enterprise Audit Log for access to certain *sensitive* systems.
3. Occasional and incidental personal use of the Internet services provided by VDSS is permitted during established lunch periods (less than 15 minutes in any continuous hour), break periods (less than 5 minutes), before and after established work schedules (less than 15 minutes in any continuous hour), provided such use does not violate LDSS, VDSS, or COV policies, procedures, or practices. This use can be further limited if it is determined to be detrimental to business use of the Internet.
4. VDSS users should avoid unnecessary use of Internet resources. With the implementation of CommonHelp and VaCMS, VDSS has become much more reliant on the network infrastructure to handle client applications for core public assistance services. Excessive use of Internet resources has been linked to network/system slowdowns, lockups, lockouts, and other issues related to various system operations.
5. Users may access personal email through Internet Service Providers (e.g., AOL, Hotmail, Exciteemail, Yahoo, Google, etc.) similar to personal calls on business phones. No attachments should be downloaded.

NOTE: The Internet is a network of interconnected computers over which VDSS has little control. The user should recognize this when using the Internet and understand that it is a public domain; the user might come into contact with information, even inadvertently, that may be considered offensive, malicious, sexually explicit, or inappropriate. The user should understand this risk during use of the Internet.

C. Network Access

1. Avoid accessing network data, files, and information not directly related to the user's job. Access to these capabilities or information does not imply permission to use this access.
2. Wireless transmissions of any data are extremely vulnerable to improper recovery or inadvertent access. Due to the relative ease in recovering these transmissions, specific security requirements are necessary. Any access not specifically addressed in the **VDSS Information Security Policy and Program Guide** is prohibited unless explicit permission is granted from the VDSS ISRM Office. VDSS users need to ensure, when accessing external wireless connections, that the session is encrypted and appropriately secured.



D. Unacceptable Use

1. In addition to unacceptable uses as defined in DHRM's Policy 1.75, Use of Electronic Communications and Social Media, the following statements, although not inclusive, define specific unacceptable uses.

Users cannot use VDSS/LDSS networks or systems to:

- Access for personal use, confidential client-specific information through SPIDeR or directly through any agency system including, but not limited to, OASIS, ADAPT, APECS/iAPECS, VEC, and/or VaCMS.
- Access sports, television (TV)/video streams and audio/video clips – related to music, TV, and movies.
- Access, download, print, or store sexually explicit material in violation of the *Code of Virginia*, [§ 2.2-2827](#).
- Knowingly upload or download commercial software in violation of its copyright and/or licensing agreement.
- Knowingly send **sensitive** data unencrypted through email.
- Forward a chain mail.
- Gamble.
- Use for product or service advertisement.
- Access data or programs to seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
- Interfere with or disrupt network users, services or equipment. Disruptions include, but are not limited to: distribution of unsolicited advertising; intentional propagation of computer viruses; and using the network to gain unauthorized entry to any other machine accessible through the network.
- Listen to radio, TV and other types of broadcasts (e.g., webcasts, streaming video) that are not related to the employee's job duties and do not have prior supervisory approval. (Written approval is required for streaming video.)
- Download or install any of the following without written authorization from the CISO:



- Copyrighted materials (e.g., music and movie files);
 - Games to include playing games over the Internet;
 - Screen savers;
 - Peer-to-Peer (P2P) file-sharing programs; and/or
 - Non-VDSS supplied software.
2. If such use interferes with the conduct of VDSS and LDSS business or job performance (based on volume or frequency), involves solicitation or illegal activities, or adversely impacts the efficient operations of the agency's computer systems, the employee's access may be limited.
 3. At no time should personal use of the Commonwealth's provided Internet services harm the agency, the Commonwealth or involve for-profit personal business.
 4. The following are provided as examples of unacceptable use: routinely visiting social networking sites such as dating sites and Twitter accounts during established work periods for personal use. At times, specific sites are blocked due to misuse; for example, Facebook and sports as a category. Please see B.3.
 5. This policy does not attempt to define all unacceptable personal use. The above information is provided as a guideline. If the employee is unclear about acceptable personal use, they should seek the advice of their supervisor, State/Local Security Officer, Director, or contact the VDSS CISO for clarification.

E. Overuse

Users should not knowingly perform actions that negatively affect the computer network or other COV/VDSS resources or that negatively affect job performance.

F. Copyright Infringement

1. Users are prohibited from using the agency's computer systems and networks to download, upload, or otherwise handle illegal or unauthorized copyrighted content.
2. All of the following activities constitute violations of this policy if done without permission of the copyright owner:



- a. Copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CDs or DVDs;
 - b. Posting or plagiarizing copyrighted material; and/or
 - c. Downloading copyrighted files that have not been legally procured.
3. This list does not include all violations; copyright law applies to many more activities than those listed above.

G. Remote Access

VDSS employees and business partners must only use approved remote access processes, devices, and procedures when connecting remotely.

H. Email Use

1. Any outbound email sent using a VDSS or LDSS email account is to be considered as equivalent to a message sent on agency letterhead. Therefore:
 - a. The content and tone of any such message must reflect the official responsibilities of the author; and
 - b. Any untrue, prejudicial, misleading, obscene, racist, sexist, or other unprofessional remarks that may make the organization liable for legal action or complaints of harassment or discrimination will be considered a breach of this policy.
2. It is prohibited to:
 - a. List a state email address for personal endeavors or personal business use;
 - b. Send an email using another's identity, an assumed name or anonymously;
 - c. Use email for the propagation of viruses, computer worms, Trojan Horses, and other malicious software; and
 - d. Use **any** outside email accounts to conduct official agency business.
3. If a suspicious email is received, delete it without opening it, and then empty the deleted mail folder.



4. Users may access their COV-provided email from any personal computer, smart phone, tablet, or other devices, using the Internet. Users who remotely access any other agency resources will use only VDSS-provided equipment that is configured, set up, and maintained by VITA or Northrop Grumman (NG) technicians without modification or similar equipment provided by a locality that is not supported by the Commonwealth's partnership with NG.
5. If an abusive, harassing, or threatening email is received, do not respond to it and report the incident to the ISRM Office at security@dss.virginia.gov.

I. Protecting Electronic Devices

To protect electronic devices:

1. Password-protect all personal computers (PCs), laptops, portable computing devices, and workstations, with the automatic activation feature set for a maximum of 15 minutes.
2. Use COV-provided encryption or other security measures to protect information stored on laptops and portable computing devices and to protect such devices from theft.
3. Make sure all PCs, laptops, and workstations contain approved virus-scanning software with a current virus database.
4. If a portable device supports virus-scanning software, make sure the software is active and that available anti-virus patches for the installed software are up-to-date.
5. The Division of Information Systems (DIS) and ISRM will disable accounts and affected devices if a remote computer or account has a virus, is party to a cyber-attack, or in some way endangers the security of the VDSS/LDSS network. Access will be reestablished once IT determines the computer, account, or device to be safe.
6. Make sure unattended portable computing devices are secured from unauthorized access. For example, make sure these devices are locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system. Logical security options include screen saver passwords and automatic session timeouts.
7. Always lock your computer when you step away from your desk.
(Ctrl + Alt + Del or Windows key + "L")
8. Use of personally-owned equipment or storage media such as scanners, USB thumb drives, compact disks, portable hard drives, smart phones, and computers to store and/or process information that has been determined to be **sensitive** is strictly prohibited and not allowed according to COV Standards. If users are unsure of the **sensitivity**, they should not process using



personally-owned devices. This requirement may be waived by VDSS during emergency situations. Any personally-owned electronic devices used (in violations of this policy) to store **sensitive** data are subject to being wiped of all data or software.

J. Protecting Data

1. Store all data files and other critical information on a network share, such as the “W:\” or “H:\” drive. These drives are backed up nightly and backups are sent off-site for disaster recovery purposes. All **sensitive** data must be stored on network drives. No **sensitive** data is to be stored on a desktop or laptop unless encrypted and approved by the CISO and the Commissioner.
2. Store media (diskettes, tapes, USBs, and CD-ROMs) in a secure location away from extreme temperature and sunlight.

K. Peer-To-Peer File (P2P) Sharing

P2P networking is not allowed on the VDSS network under any circumstances.

L. Bandwidth Use

Excessive use of VDSS bandwidth and other computer resources is not permitted. Perform large file downloads and other bandwidth-intensive tasks that can degrade network capacity or performance only during times of low usage.

M. Incidental Use

1. Occasional and incidental personal use of VDSS information resources provided by the agency is permitted, providing such use does not violate any agency or COV policies and procedures, interfere with the conduct of state business or job performance (based on volume or frequency), involve solicitation or illegal activities, adversely affect the efficient operations of the agency’s computer systems, harm the agency or the Commonwealth or involve for-profit personal business.
2. Incidental personal use of email, Internet access, fax machines, printers, copiers, etc., is restricted to approved users, and does not extend to family members or other acquaintances.



N. Use for Illegal Activities

Users must not knowingly use VDSS-owned or VDSS-provided computer systems for activities that are considered illegal under local, state, federal, or international law.

Such actions include, but are not limited to:

1. Unauthorized port scanning;
2. Unauthorized network hacking;
3. Unauthorized packet sniffing;
4. Unauthorized packet spoofing;
5. Unauthorized denial of service;
6. Unauthorized wireless hacking;
7. Any act that might be considered an attempt to gain unauthorized access to, or escalate privileges on, a computer or other electronic system;
8. Acts of terrorism;
9. Identity theft;
10. Spying;
11. Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes; and
12. Downloading, storing, or distributing copyrighted material.

O. Personal Storage Media

Personal storage devices represent a serious threat to data security and are prohibited on the VDSS network. Examples: Thumb drives, personal cloud storage, or external hard drives.



P. Flash Drives

A COV-purchased flash drive can be used to connect to a non-COV device as well as a COV device.

This practice would be appropriate with the following requirements:

- None of the work being performed on the home computer involves the use of **sensitive** data in an **unencrypted** manner. **Sensitive** data, regardless if encrypted or not, cannot be stored on the local computer's C: drive. Work performed must be accessed from and saved to the COV flash drive.
- **Sensitive** data on the flash drive must be **encrypted**.
- Non-**sensitive** data on the flash drive does not need to be **encrypted**.
- Work-related data stored on a COV purchased flash drive can be stored on or migrated to a COV device, such as a desktop or laptop computer.

Lost flash drives need to be reported to the Central Security Office. Include description of information on the drive.

Q. Software Installation

VDSS computers are set up with a standard software suite that addresses the needs of VDSS/LDSS users. If additional software needs to be installed to perform agency business (e.g., Thomas Brothers), it must meet the following requirements:

- The software must be on the VDSS Approved Software list, maintained by the ISRM Office;
- The software must be used in accordance with copyright laws and the licensing agreement;
- There must be sufficient proof of ownership;
- The software must not impact the performance of VDSS approved software or VDSS hardware; and
- The software must comply with **sensitive** data encryption in transit and at rest.

This policy applies to commercially produced software, shareware, public domain software, and freeware. The installation or modification of any software on agency information systems is prohibited unless authorized in writing by the CISO or designee. Any modification or change to the standard device or system configuration as promulgated by the VITA/NG Partnership is prohibited



unless authorized in writing by the CISO or designee. The software may be analyzed by VITA/NG to ensure the integrity of the network is maintained.

R. Information Technology (IT) Equipment and Software Purchases

1. IT hardware purchases (desktops, laptops, tablets, servers, printers, etc.) for VDSS and full support local agencies must be done by VITA. Use the Hardware Request Template in the VDSS IT Asset Management Policy and Procedures manual. Open a ticket with the VCCC and request the ticket be assigned to the VDSS IT Services Manager for approval. Shared support local agencies can purchase and maintain their own IT hardware and software in compliance with COV and VDSS requirements. VITA will review agency requests and coordinate the purchase and/or placement or seat management service assets to ensure compatibility with established device and LAN system configuration standards.
2. Media including CDs, DVDs, thumb drives, and portable hard drives if purchased by COV/VDSS monies are, by definition, COV-owned; therefore, these items can be connected and used on COV/agency equipment and networks to store and/or transport COV/agency data.

S. Acceptance and Violations of Policy

1. All users must acknowledge acceptance of, and continuing compliance with, this policy, including the *Code of Virginia*, [§ 2.2-2827](#) (Restrictions on state employee access to information infrastructure). Employees will further acknowledge that this policy may change from time to time and agree to abide by current and subsequent revisions of the policy.
2. Known instances of non-compliance with this policy should be reported to the employee's supervisor/manager, Human Resources (HR), and the VDSS ISRM Office.
3. Violations of this policy will be handled in accordance with established disciplinary procedures. Disciplinary action will be determined on a case-by-case basis by appropriate VDSS or LDSS management, with sanctions up to or including termination depending on the severity of the violation.
4. A user cannot be granted access to VDSS information systems, Internet, email, or other electronic communications before signing the **VDSS Information Security-Policy Acknowledgement** form.

