This is the combined VDSS Acceptable Use Policy including Non-Disclosure requirements and the Information Security-Policy Acknowledgment and Non-Disclosure Agreement.

VIRGINIA DEPARTMENT OF SOCIAL SERVICES

ACCEPTABLE USE POLICY

ISRM
Information Security and Risk Management

September 2023

Publication Version Control

Publication Version Control: It is the user's responsibility to ensure they have the latest version of this publication. Questions shall 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 FUSION, the VDSS 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.
Revision 5	February 2017	Updated language concerning inappropriate use of systems.
Revision 6	April 2017	VDSS employees are prohibited from using social media and Siri to conduct agency business involving ***sensitive*** case information.
Revision 7	June 2017	Updated language concerning inappropriate use of systems.
Revision 8	June 2018	Added USDA to scope. Removed SPARK. Added Thomas Brothers or Mediware Human & Social Services (formally known as Harmony). Removed NG. Verified and updated hyperlinks. Updated application nomenclature (i.e., ADAPTRO and iAPECS).
Revision 9	August 2018	Verified and updated hyperlinks.
Revision 10	September 2018	Verified and updated hyperlinks. Added Section S: Inappropriate Use of VDSS Systems and Data.
Revision 11	January 2019	Verified and updated hyperlinks. Italicized *unauthorized*. Added Disclosure Awareness. Clarified email encryption, protecting electronic devices, and flash drives.
Revision 12	February 2019	Final edits and publication.
Revision 13	April 2019	Verified and updated hyperlinks. Clarified and updated language in Email Use and Protecting Electronic Devices.

Revision 14	November 2019	Updated Section J: Protecting Data - ***Sensitive*** data including ***Personally Identifiable Information (PII)***, encrypted or unencrypted, shall **not** be stored on **Google Drive**.
Revision 15	February 2021	Verified and updated hyperlinks. Added Encryption reference to Section H Email Use.
Revision 16	March 2021	Section J: Non-***sensitive*** business critical information shall be stored 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. No ***sensitive*** data shall be stored on network drives or on a desktop or laptop unless encrypted and approved by the VDSS CISO and the Commissioner.
Revision 17	April 2022	Added sub-contractors to the scope of the policy. Added Section H. Passwords. Effective May 2022, per IRS Publication 1075, the minimum password length of fourteen (14) characters shall be enforced for information systems containing ***Federal Tax Information (FTI).*** Department of Information Services (DIS) is Information Technology Services (ITS). Section K: See Multifunction Devices (MFDs) and High-Volume Printers (HVPs): Do not print ***FTI***. If ***FTI*** is inadvertently printed, follow proper destruction and disposal of ***FTI*** procedures. See Securing Paperwork and ***Confidential*** Items o Employees must secure ***sensitive*** and ***confidential*** information in hardcopy or electronic form at the end of the day. • All ***sensitive*** and ***confidential*** paperwork must be removed from desktops and placed in a drawer or filing cabinet. (Please follow established policies and procedures on securing ***confidential*** items). • All employees must perform a brief check before leaving their workstation - securing all appropriate items and ensuring that the workstation is clean and free of unnecessary items.

		o Employees shall archive or dispose paper records as required by the applicable record retention policy. Section R: Software Use All applications whether locally installed or cloud (Internet) must be reviewed and approved by ISRM. WellSky (formally known as Mediware) Section U: ***Confidential*** information disclosed using the Virginia Employment Commission (VEC) Record Inquiry System shall be used only for purposes authorized by the VEC. Disclosure restrictions and penalties apply even ***after*** employment or contract with the agency has ended. Upon discovering a possible improper inspection or disclosure of ***FTI***, including breaches and security incidents, I must follow the proper incident reporting requirements to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving ***FTI*** within **24 hours**. Section V. Organizational Development (OD) is Human Resources (HR).
Revision 18	September 2022	Removed references to Google Drive.
Revision 19	October 14, 2022	Updated Section H. Passwords All VDSS users will utilize a ***strong password*** that: • Is at least fourteen (14) characters;
Revision 20	September 2023	Annual review. Verified and updated hyperlinks. Removed reference to AOL. Name change to Acceptable Use.

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

Identifying Significant Updates in this Document:

Vertical lines in the left margin indicate the paragraph has significant changes or additions.

PREFACE

Subject

The VDSS 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)

VDSS IT Asset Management Policy and Procedures (.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 Acceptable Use Policy***. This policy and procedure establishes the minimum requirements for the ***VDSS Acceptable Use Policy***.

Scope

This policy applies to:

All *individuals* (VDSS employees, LDSS employees, contractors, sub-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), the Virginia Employment Commission (VEC), and the United States Department of Agriculture (USDA).

Contents

A. General Statements

1. VDSS information system users shall 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 information systems will abide by COV and VDSS' policies and procedures.

4. Users shall avoid routine personal communications on electronic communication systems provided by the COV to include information 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 shall first submit their planned restrictions to the VDSS Chief Information Security Officer (CISO) for review. This augmentation shall 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 shall 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 (EAL) for access to certain ***sensitive*** information 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 shall 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 (e.g., Gmail, Outlook, iCloud, Hotmail, Yahoo!, etc.) through Internet Service Providers (similar to personal calls on business phones). No attachments shall be downloaded.

6. VDSS users are prohibited from using social media including Facebook, Twitter, Instagram, and LinkedIn to conduct agency business involving ***sensitive*** information.

   NOTE: The Internet is a network of interconnected computers over which VDSS has little control. The user shall 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 shall 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 information systems to:

   - Knowingly send ***sensitive*** data unencrypted through email.
   - Access for personal use, ***confidential*** client-specific information through SPIDeR or directly through any agency information system including, but not limited to, OASIS, ADAPTRO, 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.
   - 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 VDSS 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 information systems, the employee's access may be limited.

3. At no time shall 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 shall seek the advice of their supervisor, State/Local Security Officer, Director, or contact the VDSS CISO for clarification.

E. Overuse

Users shall 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. Passwords

H.1 Strong Passwords

All VDSS users will utilize a ***strong password*** that:

- Is at least fourteen (14) characters;
- Does not contain the user name, a real name, or VDSS;
- Does not contain a dictionary word;
- Is significantly different from previous passwords;
- Contains at least one numeric and one special character;
- Contains a mixture of at least one uppercase and one lowercase letter; and
- Cannot be reused except after 24 times using other passwords.

Note:

a. The password minimum lifetime shall be set to one day;

b. Non-privileged account passwords shall be changed at least every 90 days; and

c. Privileged account passwords shall be changed at least every 42 days.

H.2 User Password Management Responsibilities

Users of VDSS information systems:

- May not share passwords;
- May change passwords at will, but no more than once every 24 hours; and
- Must change compromised passwords.

Note: Legacy systems (i.e., ADAPTRO and iAPECS) still change passwords every 30 days.

H.3 Lost, Stolen, or Compromised Passwords

VDSS users must:

- Immediately report to the VDSS Chief Information Security Officer (CISO) the loss, theft, or compromise of passwords; and
- Immediately change their password, if compromised.

H.4 Expired Passwords and Password Resets

VDSS users must change passwords on non-privileged accounts every 90 days. VDSS users must change passwords on privileged accounts every 42 days. Legacy systems (i.e., ADAPTRO and iAPECS) still change passwords every 30 days. All accounts without activity after 90 days are locked and will require an email from supervisor indicating the account is necessary in order for a password reset. All accounts without activity after 180 days are disabled and require new Access Requests to establish access.

The “3-strikes” security feature for accounts locks a worker’s account after three (3) consecutive incorrect password attempts. The “3-strikes” feature applies to a worker’s User ID and controls access to many VDSS information systems including SAMS, VaCMS, SPIDeR, ASAPS, and MWS.

State/Local Security Officers will need to be contacted in order to reset passwords for locked accounts.

VDSS users are required to change the temporary reset password on first use.

Contact the ITS Help Desk for OASIS password resets.

Passwords can be reset by the designated State/Local Security Officers, the ITS Support Center or by emailing a request to security@dss.virginia.gov.

I. 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. Send ***sensitive*** information in an email without taking steps to encrypt the ***sensitive*** information;

    b. List a state email address for personal endeavors or personal business use;

    c. Send an email using another's identity, an assumed name or anonymously;

    d. Use email for the propagation of viruses, computer worms, Trojan Horses, and other malicious software; and

    e. 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.

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.

J. 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. Information Technology Services (ITS) 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 ITS 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. Storage, viewing, and processing of ***sensitive*** information may only be done on equipment ** or storage media ** that are Commonwealth-issued (VITA-managed), under Mobile Device Management by VITA or VDSS, or managed by shared support local agencies in adherence to VITA specified guidelines.

   **Includes scanners, USB thumb drives, optical disks, portable hard drives, smart phones, tablets, Multi-Function Devices (MFDs), printers, and computers.

   Connection of any device not issued by the Commonwealth or VDSS to the COV network or to a COV network connected device is strictly prohibited.

   Users are expressly prohibited from using Internet-connected services like Siri to conduct agency business involving ***sensitive*** information. If users are unsure of the ***sensitivity*** or the service, they shall not perform any business functions using Internet-connected services. This requirement may be waived by VDSS during emergency situations or on exception by the CISO.

   Any devices used in violations of this policy are subject to being wiped of all data and software.

Individuals performing *unauthorized* activities mentioned above will be in violation of the ***VDSS Acceptable Use Policy*** and may be subject to sanctions or disciplinary action involving loss of privileges and/or personnel actions.

9. To this end, non-COV owned devices cannot be directly connected to a COV network or a COV device, such as a desktop or laptop computer. Additionally, locality-owned devices which are not managed by VITA cannot be used to directly access a COV network or VDSS information system of record, including those information systems which contain ***sensitive*** information.

K. Protecting Data

1. Non-***sensitive*** business critical information shall be stored on a network share, such as the "W:\", "H:\", or "R:\" drives. These drives are backed up nightly, and backups are sent off-site for disaster recovery purposes. No ***sensitive*** data shall be stored on network drives or on a desktop or laptop unless encrypted and approved by the VDSS CISO and the Commissioner.

2. Store media (diskettes, tapes, USBs, and CD-ROMs) in a secure location away from extreme temperature and sunlight.

3. Multifunction Devices (MFDs) and High-Volume Printers (HVPs): Do not print ***FTI***. If ***FTI*** is inadvertently printed, follow proper destruction and disposal of ***FTI*** procedures.

4. Securing Paperwork and ***Confidential*** Items

    - Employees must secure ***sensitive*** and ***confidential*** information in hardcopy or electronic form at the end of the day.

        - All ***sensitive*** and ***confidential*** paperwork must be removed from desktops and placed in a drawer or filing cabinet. (Please follow established policies and procedures on securing ***confidential*** items).

        - All employees must perform a brief check before leaving their workstation - securing all appropriate items and ensuring that the workstation is clean and free of unnecessary items.

    - Employees shall archive or dispose paper records as required by the applicable record retention policy.

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

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

M. 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.

N. 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.

O. 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.

P. 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.

Q. 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 non-COV 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 hard drive. Work performed must be accessed from and saved to the COV flash drive. Any work using a non-COV computer which involved ***sensitive*** data must have the computer's cache memory wiped after each work session is completed on that computer.

- ***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 (CSO). Include a description of information on the drive.

R. Software Installation

All applications whether locally installed or cloud (Internet) must be reviewed and approved by ISRM.

VDSS computers are set up with a standard software suite that addresses the needs of VDSS/LDSS users. If additional software or cloud (Internet) applications need to be installed to perform agency business, 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 for installed software;
- 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, freeware, and cloud (Internet) applications. The installation or modification of any software on agency systems is prohibited unless authorized in writing by the VDSS CISO or designee. Any modification or change to the standard device or system configuration as promulgated by VITA / Third-Party Service Provider is prohibited unless authorized in writing by the VDSS CISO or designee. The software may be analyzed by VITA / Third-Party Service Provider to ensure the integrity of the network is maintained.

S. 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.

T. Inappropriate Use of VDSS Information Systems and Data

Inappropriate use of information systems to gain access to ***sensitive*** information not required to perform your job may result in the indefinite suspension of access to the information system and possible criminal referral to the local Commonwealth Attorney if the ***sensitive*** information belongs to another person. The suspension remains in force regardless of where you are employed within DSS. Access may only be restored at the discretion of the VDSS CISO.

The following would be considered ***inappropriate use***:

- Using a DSS/Federal/State information system to look up information about your family member;
- Using a DSS/Federal/State information system to look up your own information;
- Using a DSS/Federal/State information system to look up any person not part of a DSS case;
- Using a DSS/Federal/State information system to do any of the above for another co-worker or supervisor; and
- Sharing DSS data with another person/agency outside of an established Memorandum of Agreement (MOA).

U. Non-Disclosure Requirements

- Only authorized individuals shall access and/or attempt to access a DSS Restricted Area located in DSS offices where ***Personally Identifiable Information (PII)*** and/or ***Federal Tax Information (FTI)*** is received, processed, transmitted, or stored. Because these areas contain ***PII*** and/or ***FTI*** they must be treated as restricted areas.
- The penalties for *unauthorized* access and/or improper disclosure of ***FTI*** are defined in the Internal Revenue Code (IRC) 7213, IRC 7213A, and IRC 7431. Violation of these laws may result in disciplinary actions or penalties in any amount not exceeding $5,000 and/or 5 years of imprisonment. Additionally, civil penalties of not more than $1,000 and/or 1 year of imprisonment may be imposed.

- VDSS information systems and the information housed within each system including Social Security Administration (SSA)-provided information are considered assets and must be safeguarded against *unauthorized access and/or disclosure*.

- The penalties for *unauthorized* access and/or improper disclosure of SSA-provided information are defined in SSA 453 (I) (2). Violation of these laws may result in disciplinary actions or penalties in any amount not exceeding $1,000 and taxpayer civil action.

- ***Confidential*** information disclosed using the Virginia Employment Commission (VEC) Record Inquiry System shall be used only for purposes authorized by the VEC. The penalty is specified in §§ 60.2-114 and 18.2-186.6 of the Code of Virginia, whereby unlawful access or misuse of the information obtained constitutes a Class 2 misdemeanor and may be subject to civil penalties.

- Disclosure restrictions and penalties apply even ***after*** employment or contract with the agency has ended.

- Upon discovering a possible improper inspection or disclosure of ***FTI***, including breaches and security incidents, I must follow the proper incident reporting requirements to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving ***FTI*** within **24 hours**.

- Suspected incidents of *unauthorized* access and/or improper disclosure of ***FTI*** or SSA-provided information shall be reported to the VDSS CISO Barry Davis, 804-726-7153, Barry.Davis@dss.virginia.gov, and the Central Security Office (CSO), security@dss.virginia.gov, *immediately.*

V. 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 shall 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. Inappropriate use of information systems to gain access to information not required to perform your job may result in the indefinite suspension of access to the information system. The suspension remains in force regardless of where you are employed. Access may only be restored at the discretion of the VDSS CISO.

5. A user cannot be granted access to VDSS information systems, Internet, email, or other electronic communications before signing the ***VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement.***

VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement

Hand-written signatures are required.

Instructions:

The Virginia Department of Social Services (VDSS) Information Security - Policy Acknowledgement and Non-Disclosure Agreement is provided by the supervisor to new employees on the first day of employment. All new employees must read the VDSS Information Security Policy and Program Guide, the VDSS Privacy Policy and Program Manual, the VDSS Acceptable Use Policy including Non-Disclosure requirements, and Department of Human Resources (DHRM) and VDSS or Local Departments of Social Services (LDSS) Telework policies prior to signing this form. All new employees must sign the VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement prior to requesting access. The State/Local Security Officers are required to maintain electronic copies of these forms for each employee within their office/division for five to seven years. This form is to be renewed every five years.

The new user will:

A. Read the VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement.

B. Save this fillable pdf form as:
User Last name_First name_Acknowledgement_mmddyy
(For Example: Smith_Thomas_Acknowledgement_11222023).

C. Complete (type in name, date, and Division / Office / Locality on the fillable form), then, print, and sign the form to acknowledge your understanding of the VDSS Information Security Policy and Program Guide, the VDSS Privacy Policy and Program Manual, the VDSS Acceptable Use Policy including Non-Disclosure requirements, and DHRM and VDSS or LDSS Telework policies.

D. Scan the completed form to email.

E. Type the subject line as: Acknowledgement - User First name Last Name
(For example: Subject: Acknowledgement - Thomas Smith)

F. Email this completed and signed form to your supervisor.

The new user's supervisor will:

Forward the completed VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement to your State/Local Security Officer.

The State/Local Security Officer will ensure the VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement is properly completed. The State/Local Security Officer will keep an electronic copy of this form on file for each employee within their office/division for five to seven years. This form will be renewed every five years. State/Local Security Officers will be able to grant access to ***all*** of their contract employees for information systems including SAMS, SPIDeR, and VaCMS.

This form is to be retained by the State/Local Security Officer for five to seven years.
This form is to be renewed every five years.

VIRGINIA DEPARTMENT OF SOCIAL SERVICES

VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement

VDSS Information Security - Policy Acknowledgement

The Virginia Department of Social Services (VDSS) provides computers and computer accounts to its staff to assist them in the performance of their jobs. The information systems and networks belong to VDSS, and the user may use the system for authorized purposes only.

I understand that it is my responsibility as a user to read and abide by the:

- VDSS Information Security Policy and Program Guide
  http://www.dss.virginia.gov/files/division/isrm/policyguide.pdf

- VDSS Privacy Policy and Program Manual
  http://www.dss.virginia.gov/files/division/isrm/privacypolicy.pdf

- VDSS Acceptable Use Policy including Non-Disclosure requirements
  http://www.dss.virginia.gov/files/division/isrm/acceptableuse.pdf

- DHRM and VDSS or LDSS Telework policies

even if I do not agree with them. If I have any questions about the policy, I understand that I need to ask my State/Local Security Officer or contact the VDSS Central Security Office (CSO) at security@dss.virginia.gov.

I understand that any and all databases and files I have access to may have ***sensitive*** information. I understand that I am prohibited from making any *unauthorized* access or disclosure of ***sensitive*** information. I understand that I must protect data processing and telecommunication equipment, network, software, and data from accidents, misuse, and *unauthorized* use or disclosure.

I understand that violation of this agreement may result in loss of access to VDSS and Commonwealth of Virginia (COV) information systems and possible disciplinary action or prosecution if I knowingly and/or intentionally misuse any information obtained from VDSS' data processing and telecommunications equipment, network, software, or data.

I understand that VDSS has the right to monitor any and all aspects of their information systems and networks, Internet access, and email usage and that this information is a matter of public record and may be subject to inspection by the public and VDSS management. I further understand that I shall have no expectation of ***privacy*** regarding Internet usage and sites visited or emails sent or received, even if the usage was for purely personal purposes.

VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement

Non-Disclosure Agreement

Please place a check beside all items below to acknowledge you understand Non-Disclosure requirements:

☐ Only authorized individuals shall access and/or attempt to access a DSS Restricted Area located in DSS offices where ***Personally Identifiable Information (PII)*** and/or ***Federal Tax Information (FTI)*** is received, processed, transmitted, or stored. Because these areas contain ***PII*** and/or ***FTI***, they must be treated as restricted areas.

☐ The penalties for *unauthorized* access and/or improper disclosure of ***FTI*** are defined in the Internal Revenue Code (IRC) 7213, IRC 7213A, and IRC 7431. Violation of these laws may result in disciplinary actions or penalties in any amount not exceeding $5,000 and/or 5 years of imprisonment. Additionally, civil penalties of not more than $1,000 and/or 1 year of imprisonment may be imposed.

☐ VDSS information systems and the information housed within each system including Social Security Administration (SSA)-provided information are considered assets and must be safeguarded against *unauthorized* access and/or disclosure.

☐ The penalties for *unauthorized* access and/or improper disclosure of SSA-provided information are defined in SSA 453 (I) (2). Violation of these laws may result in disciplinary actions or penalties in any amount not exceeding $1,000 and taxpayer civil action.

☐ Disclosure restrictions and penalties apply even ***after*** employment or contract has ended.

☐ Upon discovering a possible improper inspection or disclosure of ***FTI***, including breaches and security incidents, I must follow the proper incident reporting requirements to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving ***FTI*** within ***24 hours***.

☐ Suspected incidents of *unauthorized* access and/or improper disclosure of ***FTI,*** VEC, or SSA-provided information shall be reported to the VDSS CISO Barry Davis, 804-726-7153, Barry.Davis@dss.virginia.gov, and the Central Security Office (CSO), security@dss.virginia.gov, *immediately.*

My signature below acknowledges my understanding of the VDSS Information Security Policy and Program Guide, the VDSS Privacy Policy and Program Manual, the VDSS Acceptable Use Policy including Non-Disclosure requirements, and DHRM and VDSS or LDSS Telework policies.

Complete this form:

User's Full Name:	Date:
Signature:	Division / Office / Locality: