VIRGINIA DEPARTMENT OF
SOCIAL SERVICES

INFORMATION SECURITY POLICY and PROGRAM GUIDE

ISRM
Information Security and Risk Management

August 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 State/Local 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	January 2019	Significant overhaul of VDSS Information Security Policy and Program Guide. Aligns with VDSS Information Security Charter. VDSS Information Resource Acceptable Use Policy includes Non-Disclosure requirements. Note changes in the VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement. Published for agency-wide review and comment.
Version 2	February 2019	Final edits. Forward to Commissioner for approval. Effective on publication to FUSION.
Version 3	April 2019	Verified and updated hyperlinks.
Version 4	October 2019	Verified and updated hyperlinks. Updated email policy. Emails that contain ***FTI*** should be properly labeled (e.g., email contains ***FTI***.) Revised Section 4.6 for end-to-end encryption and to address encryption at rest requirements. Published for agency-wide review and comment.
Version 5	November 2019	Verified and updated hyperlinks. Updated Section 4.5 Passwords. Updated Section 5 ***Information Security Incident Reporting***.
Version 6	December 2019	Updated Section 4.6 Encryption - Emailing ***Federal Tax Information (FTI)***.
Version 7	February 2020	Final edits. Forward to Commissioner for approval. Effective on publication to FUSION.
Version 8	September 2020	Verified and updated hyperlinks.
Version 9	September 2021	*IRS disclosure restrictions and penalties apply even **after** employment with the agency has ended.* Updated definitions of ***availability***, ***confidentiality***, and ***integrity***. Updated the definition of ***FTI***. Added the definition of ***Personally Identifiable Information (PII)***. Added access, inadvertent access, incidental access, *unauthorized* access, *unauthorized* disclosure, "***Need-to-Know,***" and Notification reporting. Updated ***Information Security Incident Reporting*** - added

		information spillage and definitions of data incident and data breach. Edits: Section 4.6. Encryption. VDSS users are prohibited from sending ***sensitive*** data unless the data has been encrypted. This includes data sent via email to the Help Desk or for open tickets. VDSS users are prohibited from storing ***sensitive*** data on unencrypted information systems or devices. VDSS users who must send ***PII*** via email, shall utilize either: a. VITA Virtru Email Encryption for Home Office, Regional and District Offices, and Local Departments of Social Services using Gmail (@dss.virginia.gov); or b. End-to-end email encryption services/capabilities for all Departments of Social Services **not** using Gmail (@dss.virginia.gov). If you receive an unencrypted email containing ***sensitive*** **i**nformation, notify the sender that VDSS policy requires the encryption of ***sensitive*** information that is sent over the Internet. Describe or send the individual encryption instructions so they can secure their communications with you. No ***sensitive*** information should be included in the body of the email because the email itself cannot be encrypted.
Version 10	April 2022	Sub-contractors are included in the scope of this policy. Training update: All new employees are required to complete the ***ISRM1000: New Employees curriculum*** within 30 days of employment. Updated Section 3 - Laws and Regulations: As specified in §§ 60.2-114 and 18.2-186.6 of the Code of Virginia, unlawful access or misuse of the information obtained in the **Virginia Employment Commission Record Inquiry System** constitutes a Class 2 misdemeanor and may be subject to civil penalties. Code of Virginia § 2.2-2009 - I. Information Security and

		Privacy Awareness Training requirements Section 4.1 - Role-Based Information Security and Privacy Awareness Training - added the Commissioner. Section 4.3 - Updated the definition of ***Federal Tax Information (FTI).*** Removed section 4.5 Passwords See the revised Information Resource Acceptable Use Policy. 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).*** Updated Section 4.9 - Safeguards. Added new section: 5.4 Incident Response Notification to Impacted Individuals Agency-wide review and comment.
Version 11	May 2022	Added Privacy.
Version 12	July 2022	Specific procedures removed to simplify document according to Gartner. Updated definitions of ***availability***, ***confidentiality***, and ***integrity.*** *Source: VITA glossary.* *Note: IRS disclosure restrictions and penalties apply even **after** employment or contract with the agency has ended.* Forward to the Commissioner for approval. Effective on publication to FUSION.
Version 13	October 2022	Review by Executive team. Final edits. Update to 5. ***Information Security Incident Reporting***. For ***Information Security Incidents*** that require reporting to the Virginia CyberFusion Center, VITA Commonwealth Security and Risk Management (CSRM) will report on any incidents that happened within the VITA infrastructure within **24 hours**. DSS ISRM will report any other incidents not covered by VITA within **24 hours**.
Version 14	August 2023	Verified and updated hyperlinks.

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.

Table of Contents

1. VDSS Information Security Policy and Program Guide Statement

1.1 Background

The Virginia Department of Social Services (VDSS) relies heavily on ***sensitive*** client data in agency information systems for the effective delivery of public assistance and social services programs. Rapid and continuing technical advances and need to share information have increased the risk exposure of client data. VDSS values the information, software, hardware, telecommunications, and facilities as important resources that must be protected.

1.2 Guiding Principles

The following principles guide the development and implementation of the VDSS Information Security Program:

a. Information is:

   1. A critical asset that shall be protected; and

   2. Restricted to authorized personnel for official use.

b. Information Security must be:

   1. A cornerstone of maintaining public trust;

   2. Managed to address both business and technology requirements;

   3. Risk-based and cost-effective;

   4. Aligned with VDSS priorities, prudent industry practices, and government requirements;

   5. Directed by policy but implemented by business owners; and

   6. Everybody's responsibility.

1.3 Purpose

The purpose of the VDSS Information Security Policy and Program Guide is to:

a. Promote information security and privacy awareness to individuals using VDSS information systems and information;

b. Make each user aware of their duty to safeguard personal information of clients and co-workers and protect VDSS information and information processing systems;

c. Ensure the ***confidentiality*** of VDSS and client information by protecting VDSS information systems and information against ***unauthorized*** access or disclosure;

d. Maintain the ***integrity*** of VDSS and client data by controlling who can add, modify, or delete it;

e. Meet requirements for ***availability*** of information and systems, allowing VDSS the ability to provide services and benefits to its customers;

f. Reduce the risk of data loss by accidental or intentional modification, disclosure, or destruction; and

g. Preserve VDSS rights and remedies in the event of such a loss.

Review the Information Security Program on ISRM FUSION.

2. Roles and Responsibilities

All personnel, including VDSS employees, LDSS employees, contractors, sub-contractors, volunteers, non-paid workers, student interns, business partners, and any other users of VDSS information systems and resources are responsible for the following:

a. Read and comply with the ***VDSS Information Security Policy and Program Guide***, the ***VDSS Privacy Policy and Program Plan Manual***, ***the VDSS Information Resource Acceptable Use Policy including Non-Disclosure requirements***, and related information security policies, standards, and procedures;

b. Read and sign the ***VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement*** prior to receiving access; Annually employees will electronically sign ***the VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement*** as part of the required role-based ***VDSS Information Security and Privacy Awareness Training***;

c. Do everything reasonably within their power to ensure that the ***VDSS Information Security Program*** is implemented, maintained, and enforced;

d. Report breaches of information security, actual or suspected, to their agency management and/or the VDSS Chief Information Security Officer (CISO) and the Central Security Office (CSO), security@dss.virginia.gov, immediately;

e. Take reasonable and prudent steps to protect the security and privacy of information systems and data to which they have access;

f. Complete required ***Information Security and Privacy Awareness Training*** as required within specified deadlines;

   1. The ***VDSS - ISRM1000: New Employees curriculum*** must be completed within 30 days of employment. Employees in good standing who move from one LDSS office to another LDSS office are not required to complete ***VDSS - ISRM1000: New Employees curriculum*** within 30 days of the transfer. A worker in "good standing" has no account suspensions or locks and has completed the most recent VDSS Information Security and Privacy Awareness Training.

   2. All employees must complete the ***VDSS - ISRM1030: Annual Refresher*** curriculum in less than a year (i.e., < or = 364 days) since the date of the last time s/he completed training.

   3. VDSS role-based ***Information Security and Privacy Awareness Training*** must be completed annually.

g. Encrypt ***sensitive*** data at rest and in transit. This includes ***sensitive*** client data, ***sensitive*** data about information systems, or data that could pose a risk to clients or the agency if disclosed;

h. Never share system/application credentials like User ID and password with anyone;

i. Protect ***sensitive***, client-provided hard copy data;

j. Take measures to safeguard ***sensitive*** information discussed during staff-client meetings. ***Sensitive*** discussions shall never happen in the presence of other clients or staff not working on the case.

Refer to the VDSS Information Resource Acceptable Use Policy and the VDSS Code of Ethics for further information.

Note: Versions of the VDSS Information Security Policy and Program Guide, the VDSS Privacy Policy and Program Plan Manual, the VDSS Information Resource Acceptable Use Policy, the VDSS Information Security - Policy Acknowledgment and Non-Disclosure Agreement are available on the VDSS external web server and may be shared with new employees prior to their first day of employment.

Related References:

VDSS Privacy Policy and Program Plan Manual (.pdf)

VDSS Privacy Policy and Program Plan Manual - All Personnel (Roles and Responsibilities)

VDSS Information Resource Acceptable Use Policy (.pdf)

VDSS Information Security - Policy Acknowledgement and Non-Disclosure Agreement (.pdf)

VDSS Information Security Policy and Program Guide (.pdf)

Review Roles and Responsibilities on ISRM FUSION.

3. Laws and Penalties

Privacy Act of 1974. Establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of ***Personally Identifiable Information (PII)*** about individuals that is maintained in systems of records by Federal Agencies. Provides that ***unauthorized*** access to, or disclosure of, ***PII*** in any manner to any person or agency not entitled to receive it is a misdemeanor. Violators are subject to a fine of not more than $5,000.

Internal Revenue Code (IRC 7213 7213A, and 7431). No employee of the federal, state, or local government shall unlawfully inspect and/or disclose taxpayer information. Provides that ***unauthorized*** disclosure of any information provided by the Internal Revenue Service (IRS) is a felony punishable by a fine not to exceed $5,000 or imprisonment for not more than 5 years, or both. Taxpayers may also bring civil action for damages sustained by the plaintiff as a result of such ***unauthorized*** disclosure.

*Note: IRS disclosure restrictions and penalties apply even **after** employment or contract with the agency has ended.*

Freedom of Information Act (FOIA). Establishes a "right-to-know" legal process by which requests may be made for government-held information, to be received freely or at minimal cost, barring standard exceptions. This act opens agency records to the public but requires the agency to ensure that policies and procedures are in place to review requests for information and deny release of *protected* and *sensitive* information. It provides for a civil penalty of up to $1,000 for knowing and willful violations.

Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA exists to protect the health information of citizens called Protected Health Information or PHI. The Enforcement Rule of HIPAA sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations. The Health Information Technology for Economic and Clinical Health Act (HITECH Act) extends the complete *privacy* and security provisions of HIPAA in 2009 to business associates of covered entities. VDSS and the LDSS are exempt from implementing HIPAA-related controls and requisite policies/procedures, particularly as they relate to the receipt and use of Department of Medical Assistance Services (DMAS) generated PHI.

Code of Virginia § 18.2-152.5. Computer invasion of privacy; penalties. Establishes that a person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3., relating to any other person. It is a class I misdemeanor for a DSS staff member to inappropriately access the ***sensitive*** data of any other person. It is a class 6 felony if the inappropriate access is a repeat offense, or done in the commission of any other offense.

Note: Any person who violates Code of Virginia § 18.2-152.5 and sells or distributes (discloses) such information to another is guilty of a Class 6 felony.

Virginia Employment Commission Record Inquiry System

As specified in §§ 60.2-114 and 18.2-186.6 of the Code of Virginia, unlawful access or misuse of the information obtained in the Virginia Employment Commission Record Inquiry System constitutes a Class 2 misdemeanor and may be subject to civil penalties.

Information Security and Privacy Awareness Training - Code of Virginia §2.2-2009-I.

In collaboration with the heads of executive branch and independent agencies and representatives of the Chief Justice of the Supreme Court and the Joint Rules Committee of the General Assembly, the CIO shall develop and annually update a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats. The curriculum shall include activities, case studies, hypothetical situations, and other methods of instruction (i) that focus on forming good information security habits and procedures among state employees and (ii) that teach best practices for detecting, assessing, reporting, and addressing information security threats.

Review Laws and Penalties on ISRM FUSION.

4. Information Security Program

4.1 Role-Based Information Security and Privacy Awareness Training

The ***Information Security and Privacy Awareness Training Program*** focuses on identifying risks, threats, and vulnerabilities of VDSS information systems and how to fix them. Information Security and Privacy Awareness Training will be created and delivered as role-based for the following roles: the Commissioner, Office Workers, Directors, System Administrators, State/Local Security Officers, Executive Leaders, Data Custodians, Data Owners, System Owners, and Privacy Officers. All employees are required to take at least one hour of applicable role-based Information Security and Privacy Awareness Training annually. Additional requirements apply to Administrator Account holders.

Review Awareness and Training on ISRM FUSION

4.2 *Sensitive* Data

The Commonwealth of Virginia (COV) defines ***sensitive*** data as follows:

"Any data of which the compromise with respect to ***confidentiality***, ***integrity***, and/or ***availability*** could have a material adverse effect on COV interests, the conduct of Agency programs, or the ***privacy*** to which individuals are entitled."

Data is deemed ***sensitive*** based on the following three criteria:

- ***Confidentiality*** - The protection of data from *unauthorized* disclosure to individuals or information systems.

- ***Integrity*** - The protection of data or information systems from intentional or accidental *unauthorized* modification.

- ***Availability*** - Protection of information systems and data so that they are ***accessible*** to authorized users when needed without interference or obstruction.

It is in the best interest of VDSS to ensure that data being collected, maintained, or accessed is protected. To ensure COV standards are met, it is imperative that VDSS define ***sensitive*** information in a consistent manner across all VDSS divisions/directorates/offices/districts/regions and LDSS.

The following information/data is considered "***sensitive*** information":

- Third-party ***confidential*** information (both sent and received);
- ***Personally Identifiable Information (PII)*** (anything that could be used to identify a specific person) as covered by the Government Data Collection & Dissemination Practices Act (GDCDPA);
- ***Federal Tax Information (FTI)*** that originated from the Internal Revenue Service (IRS), Social Security Administration (SSA), or U.S. Department of Labor; and
- Commissioner's working papers or correspondences used for deliberative purposes and not otherwise open to the public.

Other types of information shall be discussed with the VDSS CISO to determine the appropriate security level and how that information shall be classified.

4.3 *IRS Data*

Safeguarding ***FTI*** provided to you is critically important to ensure continuous protection of taxpayer ***confidentiality*** as required by IRC § 6103.

FTI consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control that is covered by the confidentiality protections of the IRC and subject to the IRC § 6103(p)(4) safeguarding requirements including IRS oversight.

FTI is categorized as ***Sensitive But Unclassified (SBU)*** information and may contain ***Personally Identifiable Information (PII)***.

FTI is any tax return or tax return information received from the Internal Revenue Service (IRS) or secondary source, such as the Social Security Administration (SSA), the Federal Office of Child Support Enforcement (OCSE), Bureau of Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS) or another entity acting on behalf of the IRS.

- ***FTI*** includes any information created by the agency/agency worker that is derived from return or return information received from the IRS or obtained through a secondary source.
- Access to ***FTI*** must be strictly on a ***"Need-to-Know"*** basis.
- ***FTI*** does not include information provided directly by the taxpayer or third parties. In other words, tax information received from the client (including a copy of their tax return) is not ***FTI***.
- ***FTI*** only becomes non IRS/SSA protected data when it is **overwritten** in the agency's records by another source of data, such as citizen provided.
- ***FTI*** may not be masked to change the character of information to circumvent IRC § 6103 ***confidentiality*** requirements.

Note: *VDSS applications that contain* ***FTI*** *will be periodically tested for security flaws using a web application vulnerability scanning tool, such as Acunetix or Burp Suite.*

Review ***FTI*** on ISRM FUSION.

4.4 *Personally Identifiable Information (PII)*

PII elements include:

- Name of a person with respect to whom a return is filed
- Taxpayer mailing address
- Taxpayer identification number
- Email addresses
- Telephone numbers
- Social Security Numbers
- Bank account numbers
- Date and place of birth
- Mother's maiden name
- Biometric data (e.g., height, weight, eye color, fingerprints)
- Any combination of the above

PII is any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history and criminal or employment history and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

4.5 Safeguards

A ***Safeguard Review*** is an on-site, remote, or a combination of both (hybrid) evaluation of the use of ***Federal Tax Information (FTI)*** and the measures employed by the receiving VDSS and its agents (where authorized) to protect the data.

On-site reviews: An evaluation of the security and privacy controls implemented by the agency and all supporting parties. Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.

Remote reviews: A remote evaluation of the security and privacy controls implemented by the agency and all supporting parties using secured collaborative technologies (e.g., screen-sharing capabilities, teleconferences, video-enabled software, etc.). Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.

The ***Safeguard Review*** includes all ***FTI*** received whether from the IRS or a secondary source such as SSA, Bureau of the Fiscal Service or another agency.

Safeguard Reviews are conducted to determine the adequacy of safeguards as opposed to evaluating an agency's programs. Several factors will be considered when determining the need for a review, the type of review, and the frequency of which a review will be conducted.

Safeguard Reviews are conducted on a ***three year*** cycle.

Review Safeguards on ISRM FUSION.

4.6 Security and Privacy Control Policies and Procedures

Security and privacy control policies and procedures targeted at VDSS staff who serve as or supervise System Owners, Data Owners, Data Custodians, Project Managers, Programmers, System Administrators, State/Local Security Officers, IT Developers, Contractors, Sub-Contractors, Vendors, and Infrastructure Contacts are on ISRM FUSION.

Review Security and Privacy Control Family Policies and Procedures on ISRM FUSION.

5. *Information Security Incident Reporting*

Users will ***immediately*** report any actual or suspected inappropriate access or updating of data or inappropriate disclosure of information to the **VDSS CISO Barry Davis, 804-726-7153,** Barry.Davis@dss.virginia.gov, and the **Central Security Office (CSO),** security@dss.virginia.gov.

For ***Information Security Incidents*** involving ***Federal Tax Information (FTI)***, ISRM must notify the Internal Revenue Service (IRS) Office of Safeguards including the Treasury Inspector General for Tax Administration (TIGTA) immediately but no later than **24 hours**.

For ***Information Security Incidents*** involving Social Security Administration (SSA) data, ISRM must notify the SSA within **one hour**.

For ***Information Security Incidents*** involving Virginia Employment Commission (VEC) data, ISRM must notify the VEC within **one hour**.

For ***Information Security Incidents*** that require reporting to the Virginia CyberFusion Center, VITA Commonwealth Security and Risk Management (CSRM) will report on any incidents that happened within the VITA infrastructure within **24 hours**.

DSS ISRM will report any other incidents not covered by VITA within **24 hours**.

The report shall include:

a. Name of person making the report including title and organization;

b. Information including telephone number, email, and mailing address; and

c. Brief description of the ***Information Security Incident***. Provide the name(s) of the worker(s) and client specifics involved (such as name, case number, client ID, Social Security Number (SSN), etc.). Also, please provide a description of the data involved, information systems, or applications involved, and the time period involved. Client information must be sent through encrypted email, or on an encrypted document. As much information as possible must be provided to assist in ISRM's initial assessment of the ***Information Security Incident***.

Information requested by the VDSS CISO relating to ***Information Security Incidents*** or employee access issues must be provided within 48 hours of request in a written form.

Suspected Inappropriate Use

Audit Log Request (.docx)

Confirmed Inappropriate Use

Initial Incident Reporting Form (.docx)

Review:

Incident Response Policies and Procedures on ISRM FUSION

IRS Publication 1075 (.pdf)

6. Compliance

All VDSS divisions/directorates/offices/districts/regions and LDSS are responsible for ensuring compliance with information security policies and standards. VDSS measures compliance with information security policies and standards through processes that include, but are not limited to:

- Inspections, reviews, and evaluations;
- Monitoring;
- Audits; and
- Confiscation and removal of information systems and data.

Review Compliance on ISRM FUSION.

7. Exceptions

If the Commissioner determines that compliance with the provisions of the *COV Information Security Policy* or related standards would result in a significant adverse impact to VDSS, the Commissioner may request approval to deviate from that Information Security Policy requirement by submitting a ***VDSS Information Security Policy and Standard Exception Request*** to the COV CISO.

If division/directorate/office/district/regions and LDSS management determines that compliance with the provisions of the VDSS information security policies, standards, and guidelines or related standards would result in significant adverse impact to their division/directorate/office/district/regions and LDSS, the director or senior manager may request approval to deviate from that Information Security Policy requirement by submitting a ***VDSS Information Security Policy and Standard Exception Request*** to the VDSS CISO.

Each ***VDSS Information Security Policy and Standard Exception Request*** shall be in writing and include a statement detailing the reasons for the exception and compensating controls. Requests for exception shall be evaluated and decided upon by the COV CISO or the VDSS CISO as appropriate and the requesting party informed of the action taken. Denied Exception Requests may be appealed to the COV CISO or the VDSS CISO as appropriate.

Related References

COV Information Security Program and Standard Exception Request (.doc)

VDSS Information Security Exception and Exemptions Policy (.pdf)

VDSS Information Security Exception Process (.pdf)

VDSS Information Security Policy and Standard Exception Request (.docx)

VDSS Standard Risk Exception and Acceptance Request (.docx)