VIRGINIA DEPARTMENT OF
SOCIAL SERVICES

INFORMATION SECURITY POLICY and PROGRAM GUIDE

ISRM
Information Security and Risk Management

September 2021

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 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.

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, 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 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. ***VDSS - ISRM1000: VDSS Information Security and Privacy Awareness Training*** 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 the ***VDSS - ISRM1000: VDSS Information Security and Privacy Awareness Training*** 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. 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 should 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 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 Manual (.pdf)

VDSS Privacy Policy and Program 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 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.

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: 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 preservation of authorized restrictions on information access and disclosure.

  Examples include:

  - Privacy and legal implications from improper disclosure of individual client participation in certain benefit programs, such as Temporary Assistance for Needy Families (TANF) and Supplemental Nutrition Assistance Program (SNAP), to non-VDSS/LDSS sources; and
  - Principle of *Least Privilege* for access and use is violated by worker access being provided beyond the minimum level of data, functions, and capabilities necessary to perform a user's duties.

- ***Integrity*** - The protection of information systems and information from *unauthorized* modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.

  Examples include:

  - Changing citizen-level information on clients outside of the case worker's caseload; and

- Approving benefits for a client where the same worker determined the client's eligibility (improper *Separation of Duties*).

- ***Availability*** - Timely, reliable access to information and information services for authorized users.

  Examples include:

  - The VDSS email system will not be available in a disaster if the email provider is rendered inoperative, and the email system is not backed up; and

  - Disaster Supplemental Nutrition Assistance Program (DSNAP) is required to be functional in the event of a declared emergency.

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 should be discussed with the VDSS CISO to determine the appropriate security level and how that information should be classified.

4.3 *Federal Tax Information (FTI)*

Safeguarding ***Federal Tax Information (FTI)*** is critically important to ensure continuous protection of taxpayer ***confidentiality***.

- ***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.*

4.3.1 *Personally Identifiable Information (PII)*

FTI may include ***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

4.3.2 Access

Access means when an individual: (1) enters a restricted or locked area, room, container, or system containing ***Federal Tax Information (FTI)***; or (2) obtains, acquires, receives, examines, uses, or gains knowledge of ***Federal Tax Information (FTI)***, by physical, electronic, or any other methods.

4.3.3 Inadvertent Access

Access to ***FTI*** without authority that is non-willful and unanticipated or accidental.

4.3.4 Incidental Access

Access to ***FTI*** without a "***Need-to-Know***" that may occur in extraordinary circumstances (i.e., information system failure, ***Information Security Incident Response***, disaster response).

4.3.5 *Unauthorized* Access

Unauthorized access occurs when a person gains logical or physical access to FTI without authority under IRC § 6103 and without a "***Need-to-Know***" (which would include but is not limited to agency employees with no "***Need-to-Know***" and/or janitors and security guards when there is no second barrier securing the ***FTI*** as well as developers/administrators of electronic systems/applications receiving, processing, storing or transmitting ***FTI***).

Access to ***FTI*** is permitted only to individuals who require the ***FTI*** to perform their official duties and as authorized under the IRC. ***FTI*** must never be indiscriminately disseminated, even within the recipient agency, body, or commission. Agencies must evaluate the need for ***FTI*** before the data is requested or disseminated. Inadvertent access is access to ***FTI*** without authority and is non-willful. Willful access to ***FTI*** by a person without authorization or "***Need-to-Know***" may be prosecuted under IRC § 7213A.

4.3.6 *Unauthorized* Disclosure

Unauthorized disclosure occurs when a person with access to ***FTI*** discloses it to another person without authority under IRC § 6103.

An *unauthorized* disclosure has occurred when ***FTI*** is knowingly or due to gross negligence provided to an individual who does not have the statutory right to have access to it under the IRC. Even without willfulness or gross negligence, ***FTI*** is not to be disclosed to entities or individuals who are not authorized by IRC § 6103 to have it. Inadvertent disclosure is disclosure of ***FTI*** without authority and is non-willful. Willful disclosure of ***FTI*** to a person without authorization or "***Need-to-Know***" may be prosecuted under IRC § 7213.

4.3.7 "*Need-to-Know*"

"***Need-to-Know***" is established when individuals require ***FTI*** to perform their official duties and are authorized under the IRC.

Limiting access to individuals on a "***Need-to-Know***" basis reduces opportunities to "browse" or improperly view ***FTI***. Restricting access to designated personnel minimizes improper access or disclosure. ***FTI*** disclosures must be limited to what is essential to accomplish official duties.

4.3.8 Authorized Use of *FTI*

Any agency that receives ***FTI*** for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use. If an agency needs ***FTI*** for a different authorized use under a different provision of IRC § 6103, a separate request must be sent to the Office of Disclosure.

An *unauthorized* secondary use of ***FTI*** is specifically prohibited and may result in discontinuation of disclosures to the agency and imposition of civil or criminal penalties on the responsible officials.

The Office of Safeguards validates that an agency's "need and use" of ***FTI*** conforms with the governing provisions allowing the disclosure of ***FTI***. The agency's Safeguard Security Report (SSR) must describe the purpose(s) for which ***FTI*** is collected, used, maintained, and shared.

4.3.9 Disclosure of *FTI* to Non-Paid Employees

VDSS users will not grant access or disclose ***FTI*** to non-paid employees such as student interns, volunteers, or any other type of non-paid employee.

4.3.10 Disclosure of *FTI* to Benefit Programs Contractors

No officer or employee of any federal, state, or local agency administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or Title 38, United States Code, or certain housing assistance programs is permitted to make further disclosures of ***FTI*** for any purpose.

Human services agencies may not contract for services that involve the disclosure of ***FTI*** to contractors. For accessing ***FTI***, the Internal Revenue Service (IRS) considers workers to be either employees or contractors. An employee is a worker that receives a W2 issued by the locality or State. The IRS considers everyone else a contractor as far as accessing ***FTI*** is concerned. This definition includes interns, volunteers, and VIEW workers, as well as workers that receive a 1099. Everyone falling under this broad definition of a contractor is prohibited from accessing ***FTI***.

4.3.11 Access by DCSE Contractors

In general, no officer or employee of any state and local child support enforcement agency can make further disclosures of ***FTI***.

However, limited information may be disclosed to agents or contractors of the agency for the purpose of, and to the extent necessary in, establishing and collecting child support obligations and locating individuals owing such obligations.

The information that may be disclosed for this purpose to an agent or a contractor is limited to:

- The address;
- Social Security Number (SSN) of an individual with respect to whom child support obligations are sought to be established or enforced; and
- The amount of any reduction under IRC 6402(c) in any over payment otherwise payable to such individual.

Tax refund offset payment information may not be disclosed by any federal, state, or local child support enforcement agency employee, representative, agent, or contractor into any court proceeding. To

satisfy the re-disclosure prohibition, submit the payment date, whether the payment is voluntary or involuntary, and the payment amount for all payment sources (not just tax refund offset payments) into court proceedings.

4.3.12 Commingling of *FTI*

Commingling of ***FTI*** refers to having ***FTI*** and non- ***FTI*** data residing on the same paper, electronic media, or data center.

- ***FTI*** must be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures;
- Agencies should attempt to avoid maintaining ***FTI*** as part of their case files;
- In situations where physical separation is impractical, the file must be clearly labeled to indicate that ***FTI*** is included, and the file must be safeguarded; and
- All ***FTI*** must be removed prior to releasing files to an individual or agency without authorized access to ***FTI***.

4.3.13 Notification Reporting

IRC § 6103 limits the usage of ***FTI*** to only those purposes explicitly stated. Due to the security and privacy implications, higher risk of unauthorized disclosure and potential for *unauthorized* use of ***FTI*** based on specific activities conducted, the Office of Safeguards requires advanced notification of at least **45 days** prior to implementing certain operations or technology capabilities that require additional uses of the ***FTI***.

Prior to…	Requirement
Implementing Cloud Computing	√ Submit Notification
Disclosure to a Contractor or Sub-Contractor	√ Submit Notification
Re-disclosure by Contractor to Sub-Contractor	√ Submit Notification and receive approval
Using ***FTI*** in Tax Modeling for Tax Administration	√ Submit Notification and receive approval
Using ***FTI*** in Test Environment	√ Submit Notification and receive approval

For information on ***FTI*** in transit, faxing ***FTI***, emailing ***FTI***, ***FTI*** and multi-functional devices, and destruction and disposal of ***FTI***, review ***FTI*** on ISRM FUSION.

4.4 Data Sharing

Data held by, or provided to, the VDSS must be properly managed and protected. To this end, data which VDSS shares with other organizations or receives to administer benefits and services must be controlled in a manner which meets security requirements.

Users may only share data with an approved data sharing arrangements, either by Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), contract, use agreement, or any such mechanism. The data sharing arrangement must be approved by the VDSS Chief Information Security Officer (CISO) prior to any data movement or receipt. This includes data shared with other state and local agencies, their contractors, sub recipients, and the like. Similarly, the process by which the data will be transported, stored, and destroyed, as appropriate, must also be approved by the VDSS CISO.

- Agencies and subdivisions within an agency may be authorized to obtain the same ***FTI*** for different purposes, such as a state tax agency administering tax programs and a component human services agency administering benefit eligibility verification programs (IRC 6103[l][7]) or child support enforcement programs (IRC 6103[l][6]). However, the IRC disclosure authority does not permit agencies or subdivisions of agencies to exchange or make subsequent disclosures of this information for another authorized purpose even within the agency.

- In addition, unless specifically authorized by the IRC, agencies are not permitted to allow access to ***FTI*** to agents, representatives, or contractors.

- Any data sharing requests outside of the above framework may need to follow Freedom of Information Act (FOIA) procedures.

- ***FTI*** cannot be shared.

- Data must only be shared for purposes consistent with federal or state regulations.

- ***FTI*** shall not be accessed by agency employees, agents, representatives, or contractors located offshore - outside of United States territories, embassies, or military installations.

- Further, ***FTI*** may not be received, processed, stored, transmitted, or disposed of by information systems located offshore.

- The agency must restrict the sharing/re-disclosure of ***FTI*** to only those authorized in IRC 6103 and as approved by the IRS Office of Safeguards.

NOTE: No Department of Motor Vehicles (DMV) data, information, photographs or other items sourced from DMV can be stored, kept, or otherwise uploaded to any system. This includes data not only obtained directly from DMV via the IBM mainframe, but also any DMV data produced via SPIDeR.

DMV data provided by the client or their designee, such as a driver license, driver record, government photo ID, or any other data provided by the client to VDSS for program or service eligibility determination or for case or client management purposes is deemed to not be sourced from DMV directly. As such, any

and all data provided by the client or their designee may be stored, kept, or otherwise uploaded to any system of record.

4.5 Passwords

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

- Is at least eight (8) 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.

Review Password Management on ISRM FUSION.

4.6 Encryption

VDSS users must encrypt ***sensitive*** information [e.g., ***Personally Identifiable Information (PII)*** and ***Federal Tax Information (FTI)***] in emails prior to transmission. ***Sensitive*** information must also be encrypted while stored on any information system or device.

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).

End-to-end email encryption ensures that only the intended recipient of the message can read the contents. Most email providers do not encrypt email to this standard by default.

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.

a. ***FTI*** should only be transmitted to authorized individuals with a "***Need-to-Know***."

b. Emails that contain ***FTI*** should be properly labeled (e.g., email contains ***FTI***.)

c. Mail server and network equipment supporting the email infrastructure must be hardened and protected against malware.

d. Audit trails shall capture relevant events.

e. Webmail access from points external to the agency must be controlled.

4.7 Account Management

The State/Local Security Officer should suspend the account for all personnel including VDSS employees, LDSS employees, contractors, volunteers, non-paid workers, student interns, and business partners any time they will be gone for more than 30 calendar days.

Employees on leave 90 to 179 calendar days require an email to reset the account; the email must come from the person(s) who approved the original Access Request.

State/Local Security Officers should terminate system access for employees on leave 180 calendar days or more. New Access Requests must be submitted upon return.

Note: Circumstances including Family Medical Leave Act (FMLA), short-term disability, long-term disability, and military leave may be considered on a case-by-case basis with coordination between the employee's supervisor and Organizational Development (OD).

More procedural details:

- From onset to 30 days of absence - If it is known that the employee will be gone for an extended amount of time, then the State/Local Security Officer should suspend the accounts with approval to do so provided by the employee's supervisor.

- 31-89 days of absence - If the suspension has not been done prior to 30 days, the suspension must occur after the 30-day window has been eclipsed. The suspension action can be done without prior approval.

- 90-179 days of absence - Reactivation requires a formal email to be received from the person(s) who approved the original Access Request or the agency director, as appropriate.

- 180 days or more of absence - Employee access should be terminated across all accounts. New Access Requests must be submitted upon return.

To the extent practicable, the decisions and actions necessary prior to the employees' absence regarding their emails must be done and completed by the State/Local agency.

The Central Security Office (CSO) only suspends accounts at the direction of the Director/District Manager with exceptions made in the absence of the Director/District Manager.

4.8 Safeguards

The ***Safeguard Review*** is an evaluation of the use of ***Federal Tax Information (FTI)*** received from the Internal Revenue Service (IRS), the Social Security Administration (SSA), or other agencies and the measures employed by the Virginia Department of Social Services (VDSS) to protect that data.

Review Safeguards on ISRM FUSION.

4.9 Security Control Policies and Procedures

Security Control policies and procedures targeted at VDSS staff who serve as or supervise Data Owners, Data Custodians, Project Managers, System Owners, Programmers, System Administrators, and Security Officers are on ISRM FUSION.

Review Security 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.

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)

5.1 Information Spillage

Information spillage refers to instances where ***FTI*** is inadvertently placed on systems that are not authorized to handle ***FTI*** or are not part of the agency's intended ***FTI*** workflow. Upon discovery, Corrective Action is required to remove the ***FTI*** from the unintended system and ensure there were no *unauthorized* accesses or disclosures. If the agency successfully contains the spill and ensures there were no indicators of further incident or compromise, there is no need to report the spill to the Office of Safeguards or TIGTA.

5.2 Data Incident

A **data incident** is an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the ***integrity***, ***confidentiality***, or ***availability*** of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies.

An incident involving the loss or theft of an IRS asset containing ***FTI***, or the loss or theft of a physical document that includes ***FTI***, or the inadvertent *unauthorized* disclosure of ***FTI***, is known as a **data breach**. See the **data breach** definition below. Often, an occurrence may be first identified as an incident, but later identified as a **data breach** once it is determined that the incident involves ***FTI***. This is often the case with a lost or stolen laptop or electronic storage device.

5.3 Data Breach

A **data breach** is a type of incident involving a loss, theft, or inadvertent *unauthorized* disclosure of ***FTI***.

A **data breach** is defined as the loss of control, compromise, *unauthorized* disclosure, *unauthorized* acquisition, or any similar occurrence where:

- A person other than an authorized user accesses or potentially accesses ***FTI*** or,
- An authorized user accesses or potentially accesses ***FTI*** for an other than authorized purpose.

A **data breach** is not limited to an occurrence where a person other than an authorized user potentially accesses ***FTI*** by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A **data breach** may also include the loss or theft of physical documents that include ***FTI*** and portable electronic storage media that store ***FTI***, the inadvertent disclosure of ***FTI*** on a public website or an oral disclosure of ***FTI*** to a person who is not authorized to receive that information. It may also include an authorized user accessing ***FTI*** for an other than authorized purpose.

Some common examples of a **data breach** include:

- A laptop or portable storage device storing ***FTI*** is lost or stolen.
- An email containing ***FTI*** is inadvertently sent to the wrong person.
- A box of documents with ***FTI*** is lost or stolen during shipping.
- An *unauthorized* third party overhears agency employees discussing ***FTI***.
- A user with authorized access to ***FTI*** sells it for personal gain or disseminates it.
- ***FTI*** is posted inadvertently on a public website.
- An information system that maintains ***FTI*** is accessed by a malicious actor.

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)