



Prepared By:
Information Security and Risk Management



Document Prepared:
September 2012

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 in the Division of Finance (DOF). The VDSS CISO will issue an Agency-wide Broadcast and post the revised publication version on the [Services.Programs.Answers.Resources.Knowledge \(SPARK\) Intranet](#), and provide an e-mail announcement to division/directorate/office/district/regions and Local Departments of Social Services (LDSS) Information Security Officers (SOs) as well as other parties the VDSS CISO considers to be interested in the change.

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

Version	Date	Comments
Original	July 15, 1992	
Revision 1	April 3, 2001	
Revision 2	November 18, 2003	
Revision 3	May 2007	
Revision 4	May 2008	
Revision 5	April 2012	
Revision 6	August 2012	Final reviews complete. Forward to Agency Head for approval. Effective upon publication to SPARK.
Revision 7	September 4, 2012	Final changes and new Non-Paid Employee, Seasonal Worker status added.

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

PREFACE

Subject

The *VDSS Written Information Security Program*

Effective Date: October 15, 2012

Compliance Date: January 1, 2013

Authority

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

[TANF Manual 103.1 \(1/20/97\)](#), Purpose of Safeguarding of Information and Scope of Regulations

VDSS/DCSE Manual, Chapter 2 (11/1/96), Confidentiality/Information Release

HHS 45 CFR 303.21 and 45 CFR 303.105

[IRS Revenue Procedure Section 6103 \(L\)\(7\)\(b\)](#), Disclosure of Information to Federal, State, and Local Agencies

[IRS Publication 1075](#) (.pdf)

[ITRM Standard SEC501-06](#) (.pdf)

[Social Security Program Rules](#)

USDA/FNS 7 CFR 72.1 (c), 27.1 (d), Disclosure of Information

Code of Virginia [Social Service Laws 63.2](#) (2002)

Purpose

To define the *VDSS Information Security Program*.

Scope

This policy applies to:

All *Individuals* (VDSS employees, LDSS employees, contractors, vendors, volunteers, work experience personnel and other persons and organizations) who have a need to use VDSS-related information or information processing systems;

All information and information processing systems associated with VDSS; and

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

In accordance with the *Code of Virginia* § [2.2-603](#), § [2.2-2009](#), and § [2.2-2010](#) VDSS is responsible for complying with Commonwealth Information Technology Resource Management (ITRM) policies and standards and considering Commonwealth ITRM guidelines issued by the Commonwealth of Virginia (COV) Chief Information Officer (CIO). In addition: “The director of every department in the executive branch of state government shall report to the CIO as described in § [2.2-2005](#), all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's IT systems with the potential to cause major disruption to normal Agency activities. Such reports shall be made to the CIO within 24 hours from when the department discovered or should have discovered their occurrence.”

Table of Contents

1. Information Security Program Statement.....	1 -
1.1 Background.....	1 -
1.2 Guiding Principles.....	1 -
1.3 Purpose.....	1 -
1.4 Statement of Program.....	2 -
2. Roles and Responsibilities.....	3 -
2.1 Policy.....	3 -
2.2 Commissioner.....	3 -
2.3 Chief Information Security Officer (CISO).....	3 -
2.4 Information Security and Risk Management (ISRM) Office.....	4 -
2.5 Security Officers (SOs).....	4 -
2.6 Management.....	5 -
2.7 System Owner (VDSS Division Directors (DDs) and their designees).....	5 -
2.8 Data Owner (DO).....	6 -
2.8.1 VDSS DDs and their designees.....	6 -
2.8.2 Local Social Service Agency Directors (LSSADs).....	6 -
2.9 All Personnel.....	7 -
3. Laws and Penalties.....	8 -
3.1 Laws.....	8 -
3.2 Penalties.....	8 -
4. Information Security Program.....	10 -
4.1 Risk Management (RM).....	10 -
4.1.1 Sensitive Data Definition.....	11 -
4.1.2 Business Impact Analysis.....	13 -
4.1.3 Risk Assessment (RA).....	13 -
4.1.4 Security Audits.....	14 -
4.2 Continuity Planning (CP).....	14 -
4.2.1 Emergency Response Plans.....	15 -
4.2.2 Business CP.....	15 -
4.2.3 IT Disaster Recovery (ITDR) Plans.....	15 -
4.2.4 IT System and Data Backup and Restoration Plans.....	16 -
4.3 Information System Security Plans.....	16 -
4.4 Information Systems Interoperability Security.....	16 -
4.5 IT System Application Security.....	17 -
4.6 Remote Access.....	17 -
4.6.1 Single-factor authentication (SFA).....	17 -
4.6.2 Dual-factor authentication (DFA).....	17 -
4.6.3 Password Requirements for Dual Factor Token PIN.....	18 -

4.7 Wireless Security	- 18 -
4.7.1 Guest Wireless	- 18 -
4.7.2 Wireless for VDSS systems	- 19 -
4.7.3 Wireless from Home or other Public Places	- 19 -
4.7.4 Wireless in Local Offices.....	- 20 -
4.8 Mobile Devices	- 20 -
4.9 Logical Access Control	- 20 -
4.9.1 Account Management	- 21 -
4.9.1.1 Non-Paid Employees	- 21 -
4.9.1.2 Seasonal Worker	- 21 -
4.9.1.3 Approval Process Flow for VDSS Security Forms	- 22 -
4.9.2 Password Management	- 23 -
4.10 Data Protection.....	- 24 -
4.10.1 ISRM Safeguards Program (SP)	- 26 -
4.10.2 Data Storage Media Protection	- 26 -
4.10.3 Encryption.....	- 27 -
4.11 Facilities Security	- 27 -
4.12 Personnel Security.....	- 28 -
4.13 Logical Access Determination and Control	- 28 -
4.14 Third-Party/Contractor Requirements	- 28 -
4.14.1 Equipment and Software Ownership	- 30 -
4.14.2 Reporting	- 30 -
4.14.3 Incident Reporting	- 30 -
4.15 Security Awareness Training Program (SATP)	- 31 -
4.16 Acceptable Use	- 32 -
4.17 Asset Management	- 33 -
4.17.1 Asset Control	- 33 -
4.17.2 Software License Management	- 33 -
4.17.3 Configuration Management and Control	- 34 -
5. Compliance.....	- 35 -
5.1 Monitoring	- 35 -
5.1.1 General Monitoring Activities	- 35 -
5.1.2 Requesting and Authorizing Monitoring	- 36 -
6. Process for Requesting Exception to the Information Security Policy	- 36 -

1. *Information Security Program Statement*

1.1 Background

The Virginia Department of Social Services (VDSS) relies heavily on the application of information technology for the effective delivery of public assistance and social services programs. Rapid and continuing technical advances have increased the dependence of state and local Agencies on information systems. The value of VDSS information, software, hardware, telecommunications, and facilities is an important resource and must be protected.

1.2 Guiding Principles

The following principles guide the development and implementation of VDSS Information Security Management and Practices (ISMPs):

- 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 Program* is to:

- a. *Promote information security awareness to individuals using VDSS systems and information;*
- b. *Make each user aware of their duty to protect VDSS information and information processing systems;*

- c. Ensure the *confidentiality*, *availability*, and *integrity* of data;
- d. Reduce the risk of data loss by accidental or intentional modification, disclosure, or destruction; and
- e. Preserve VDSS rights and remedies in the event of such a loss.

1.4 Statement of Program

The Commissioner is responsible for the security of VDSS data including case records and documents containing client or *confidential/sensitive* information; and for taking appropriate steps to secure VDSS Information Technology (IT) systems and data through the *VDSS Information Security Program*. This program and related policies and standards provide the minimum security requirements that apply to all division/directorate/office/district/regions and Local Departments of Social Services (LDSS). Effective security is a team effort involving the participation and support of every user who interacts with VDSS data and information systems. It is the responsibility of every user to know these policies and to conduct their activities accordingly. Exceptions to this program and related policies and standards must be clearly documented, reviewed, and approved by the Commissioner or the VDSS CISO as appropriate.

The function of this program is to protect VDSS information assets from creditable threats, whether internal or external, deliberate or accidental. It is the policy of VDSS to use all reasonable security control measures to:

- a. Ensure the *confidentiality* of VDSS information by protecting VDSS information and information systems against unauthorized access or disclosure;
- b. Maintain the *integrity* of VDSS data by controlling who can add, modify or delete it;
- c. Meet requirements for *availability* of information and information systems, allowing VDSS the ability to provide services and benefits to its customers;
- d. Meet federal, state, and other regulatory and legislative requirements; and
- e. Ensure business continuity in the event of any type of business interruption.

Violations of this policy must be reported to the appropriate VDSS division/directorate/office/district/regions and/or LDSS Security Officers (SOs), LDSS Directors (LDSSDs) and the VDSS CISO. Depending on the severity, an employee who violates these policies may receive a Standards of Conduct notice. Violations of state and local laws will be reported to the appropriate law enforcement authorities. Prosecuting action may be undertaken if a person knowingly and intentionally violates any local, state, or federal laws or uses any VDSS-related information, information processing systems or equipment for fraudulent, extortive, or destructive purposes.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure, or destruction of data and information systems. This also includes accidental loss or destruction. In the case of lost or missing computer equipment or software, notification must also be made immediately to the VDSS CISO.

Related References:

[Commonwealth of Virginia Information Security Policy & Standard Exception Request \(.doc\)](#)

[Standards of Conduct, Department of Human Resource Management \(.pdf\)](#)

2. Roles and Responsibilities

2.1 Policy

VDSS and LDSS must have an effective security administration function in place. For an ***Information Security Program*** to be effective, someone in each VDSS division/directorate/office/district/region and LDSS should be assigned the responsibility for administering the security program in their unit. The individual selected should be cognizant of data processing and information security fundamentals and possess sufficient abilities to understand, implement and enforce Information Security Policies and Procedures (ISPPs).

VDSS has distributed security architecture. There are approximately 150 state and local VDSS offices located throughout the Commonwealth. Each VDSS and LDSS must designate a SO and at least one backup SO whose responsibility is to ensure compliance with the VDSS Information Security Policies and Standards (ISPPs). The SOs are responsible for administering the users within their respective offices to include adding, removing users and modifying access privileges. The VDSS Information Security and Risk Management (ISRM) Office oversees the ***VDSS Information Security Program*** and provides administration for primary SOs and their backups.

2.2 Commissioner

The Commissioner is responsible for the security of the VDSS IT systems and data including case records and documents containing client or ***confidential*** information. The Commissioner, through the ISRM Office, is responsible for assuring that the ***VDSS Information Security Program*** is developed and distributed to all VDSS division/directorate/office/district/regions and LDSS staff, contractors, vendors, and other persons and organizations that have a need to use VDSS-related information and information processing systems. The Commissioner is responsible for final interpretation of this policy.

2.3 Chief Information Security Officer (CISO)

The CISO is responsible for developing and managing the ***VDSS Information Security Program***. The CISO duties are as follows:

- a. Develop and manage an ***Information Security Program*** that meets or exceeds the requirements of Commonwealth of Virginia (COV) IT security policies and standards in a manner commensurate with risk;

- b. Develop and maintain a Security Awareness Training Program (SATP) for VDSS division/directorate/office/district/regions and LDSS staff, including contractors, volunteers and service providers;
- c. Coordinate and provide IT security information to the COV CISO as required;
- d. Implement and maintain the appropriate balance of protective, detective, and corrective controls for VDSS IT systems commensurate with data sensitivity, risk, and system criticality;
- e. Mitigate and report all IT security incidents in accordance with the *Code of Virginia* § [2.2-603](#), the Virginia Information Technologies Agency (VITA), and federal requirements and all other applicable obligations and take appropriate actions to prevent recurrence;
- f. Maintain liaison with the COV CISO; and
- g. Verify and validate that all VDSS IT systems and data are classified for *sensitivity*.

2.4 Information Security and Risk Management (ISRM) Office

The VDSS ISRM Office is responsible for providing technical information, security assistance, and fostering and overseeing the *VDSS Information Security Program*. Specific responsibilities include but are not limited to:

- a. Provide technical assistance to VDSS division/directorate/office/district/regions and LDSS in developing, implementing, and administering their security programs and procedures;
- b. Develop, maintain, and disseminate Information Security Policies, Standards and Guidelines (ISPSGs), ensuring their uniform interpretation and implementation throughout VDSS division/directorate/office/district/regions and LDSS;
- c. Participate in VDSS system development activities to ensure an appropriate level of security, *confidentiality* and *availability* is provided to VDSS systems;
- d. Assist business areas to conduct Business Impact Analyses (BIAs) and Risk Assessments (RAs) for VDSS IT systems;
- e. Review security incident reports and coordinating Corrective Actions (CAs) to prevent a similar occurrence; and
- f. Investigate alleged security breaches.

2.5 Security Officers (SOs)

Division/directorate/office/district/regional and LDSS SOs serve as the Point of Contact (POC) for all security-related matters. SOs are empowered by their director to make decisions regarding the protection of VDSS information, resources, and user access privileges to ensure VDSS information and resources are protected from misuse or abuse. SOs are responsible to:

- a. Administer user access privileges to VDSS information systems and resources;
- b. Verify the access privileges of active employees;
- c. Communicate security-related events to the VDSS CISO;
- d. Ensure local staff complete the IT Security Awareness and Federal Safeguards Training courses annually.

Related Reference:

See Approval Process Flow for DSS Security Forms – Section 4.9.1 Account Management

2.6 Management

Managers at all levels are responsible for the security of VDSS IT systems and data including case records and documents containing client or *confidential* information under their jurisdiction. They shall take all reasonable actions to provide adequate security and to escalate problems, requirements, and matters related to information security to the highest level necessary for resolution.

Division/directorate/office/district/regional management and LDSSDs' responsibilities are to:

- a. Appoint SOs and backup SOs;
- b. Implement and enforce procedures within their units which ensure compliance with VDSS ISPSs;
- c. Ensure violations or suspected violations of VDSS ISPs are reported to the VDSS CISO; and
- d. Ensure that all users of VDSS information and information systems are made aware of VDSS ISPSs and receive continuing security training.

2.7 System Owner (VDSS Division Directors (DDs) and their designees)

The System Owner is the VDSS manager responsible for making system-related development and maintenance decisions and establishing priorities. With respect to IT security, the System Owner's responsibilities include the following:

- a. Require that all IT system users complete the required SATP activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter;
- b. Manage system risk and develop any additional ISPSGs required to protect the system in a manner commensurate with risk;
- c. Maintain compliance with VDSS ISPSGs in all IT system activities;
- d. Maintain compliance with requirements specified by Data Owners (DOs) for the handling of data processed by the system; and

- e. Designate a System Administrator (SA) for the system if the system is not administered by the Information Technology Partnership (ITP) - currently Northrop Grumman.

2.8 Data Owner (DO)

2.8.1 VDSS DDs and their designees

The DO is the VDSS manager responsible for the policy and practice decisions regarding data including case records and documents containing client or *confidential* information. The DO is responsible for the following:

- a. Evaluate and classify *sensitivity* of the data with the assistance of the CISO;
- b. Define protection requirements for the data based on the *sensitivity* of the data, any legal or regulatory requirements, and business needs with the assistance of the CISO;
- c. Communicate data protection requirements to the System Owner; and
- d. Define requirements for access to the data.

2.8.2 Local Social Service Agency Directors (LSSADs)

LDSSDs that enter data supplied by VDSS into local systems are responsible for the security of the local IT systems and data contained therein. The local director is responsible for assuring that ISPs are developed and distributed to all LDSS staff, contractors, vendors, and other persons and organizations that use local systems that process or store VDSS-provided information. The local director is responsible for final interpretation of local ISPs and will provide to the VDSS ISRM Office copies of all local ISPs.

The local director's data ownership responsibilities include:

- a. Establish and maintain an *Information Security Program* for local systems that process or store VDSS- provided information (i.e., Harmony, EZ-filer) that includes:
 - o Develop and distribute ISPSs to all individuals who use local systems that process or store VDSS- provided information; and
 - o Establish and provide a SATP relevant to local systems.
- b. Provide for both physical and logical separation of duties by ensuring no one person has sole control of *sensitive* processes.

2.9 All Personnel

All personnel, including VDSS employees, LDSS employees, contractors, volunteers, business partners, and any other users of VDSS information systems and resources are responsible for the following:

- a. Read the ISPSs;
- b. Read and sign the *Acceptable Use Awareness Acknowledgement* document;
- c. Comply with VDSS ISPs;
- d. Do everything reasonable within their power to ensure that the *VDSS Information Security Program* is implemented, maintained, and enforced;
- e. Report breaches of information security, actual or suspected, to the VDSS CISO and to appropriate management; and
- f. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

3. Laws and Penalties

3.1 Laws

Privacy Act of 1974. Establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of Personal 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 & 7431). No employee of the federal, state, or local government shall unlawfully inspect and/or disclose of 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.

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. 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 exempted 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 Protected Health Information (PHI).

3.2 Penalties

Employees who violate the Information Security Policy may be subject to a Standard of Conduct offense. Violations by others may result in actions which Executive Management deems appropriate. VDSS cooperates with law enforcement Agencies in the investigation and prosecution of any violations of these laws.

Related References:

[Code of Virginia § 2.2-3700 et seq.](#) –FOIA

[Code of Virginia § 2.2-3803.](#) - Administration of systems including personal information; Internet privacy policy; exceptions

[Code of Virginia § 2.2-3806.](#) – Rights of data subjects

[Code of Virginia § 2.2-3815.](#) - Access to social security numbers prohibited; exceptions.

[Code of Virginia § 63.2.](#) – Welfare (Social Services)

[Code of Virginia § 63.2-102.](#) - Allowing access to records and information for public assistance programs and child support enforcement; penalty.

[Code of Virginia § 63.2-405.](#) - Provisions for determination of eligibility for medical care and medical assistance; provision of social services; regulations.

[Code of Virginia § 63.2-501.](#) – Application for assistance.

[Federal Code § 7 CFR 272.1\(c\);](#) - Disclosure

[Federal Code § 42 CFR 431.305.](#) – Types of information to be safeguarded

[Federal Code § 42 CFR 431.306.](#) – Release of information

[Federal Code § 42 CFR 433.138.](#) – Identifying Liable Third Parties

[Federal Code § 45 CFR 303.21](#) – Administration for Children & Families

[Federal Code § 303.105](#) - Procedures for making information available to consumer reporting agencies

[Health Insurance Portability and Accountability Act \(HIPPA\) of 1996.](#) (.pdf)

[IRS Revenue Procedure Section 6103 \(L\)\(7\)\(b\),](#) Disclosure of Information to Federal, State, and Local Agencies

[IRS Publication 1075](#) (.pdf) – Tax Information Security Guidelines for Federal, State and Local Agencies

[Internal Revenue Code: Sec. 7213.](#) – Unauthorized disclosure of information

[Internal Revenue Code: Sec. 7431.](#) – Civil damages for unauthorized inspection or disclosure of returns and return information

[ITRM Standard SEC501-06](#) (.pdf)

[Privacy Act of 1974 5 U.S.C. § 552a.](#)

[Social Security Program Rules](#)

[Standard of Conduct, Department of Human Resource Management](#) (.pdf)

[TANF Manual 103.1 \(1/20/97\),](#) Purpose of Safeguarding of Information and Scope of Regulations

USDA/FNS 7 CFR 72.1 (c), 27.1 (d), Disclosure of Information

VDSS/DCSE Manual, Chapter 2 (11/1/96), Confidentiality/Information Release

[VDSS Medicaid Manual](#) (.pdf)

[Virginia Administrative Code 12VAC30-20-90](#). – Confidentiality and disclosure of information concerning Medicaid applicants and recipients

4. Information Security Program

Security programs must include protective measures and procedures to ensure that the appropriate levels of ***confidentiality***, ***integrity***, and ***availability*** of data, information, and systems are sustainable. The specific structure of an Agency's information technology security program will vary depending on the scope and nature of the information technology resources and ***sensitive*** information for which the Agency is responsible.

A good security program should include documented policies and procedures that support the mission of the Agency and is derived from industry best practices, and if applicable, the security policies and standards of the COV and the federal government.

The VDSS CISO is charged with developing and administering the ***VDSS Information Security Program*** in a manner that meets VDSS business needs, protects IT systems and data in a manner commensurate with data ***sensitivity*** and risk, and, at a minimum, meets the requirements of COV IT policies and standards. VDSS requirements for the implementation of following the ***Information Security Program*** requirements can be found in ***VDSS Information Security Standards***. While the majority of these security program components are the responsibility of VDSS, infrastructure-related components are the responsibility of the VITA/Northrop Grumman (NG) partnership.

4.1 Risk Management (RM)

RM is the process of identifying and ensuring the protection of information and data received, processed, shared, and stored by VDSS that is defined as ***sensitive***.

COV requires all Agencies to evaluate Agency-owned IT systems that contain ***sensitive*** data at least once every three years via an IT RA. The RA should evaluate risks and vulnerabilities and adopt mitigation steps (processes, procedures, hardware, software, etc.) to manage or minimize the risks or formally accept them if unable to mitigate. There are three major areas of protection required by COV:

- ***Confidentiality*** - the impact of unauthorized disclosure;
- ***Integrity*** - the impact of unauthorized modification of data; and
- ***Availability*** - the impact of outages or system unavailability.

Section 4.1.1 of this document discusses the ***Sensitive Data Definition***.

Due to the large number of individual systems owned by the same owner and the resources needed to complete RAs, VDSS will combine the RA process into the modifications of those systems. The ISRM Office reviews the proposed changes and existing information and provides a RA of the new system and related changes. These recommendations are documented in both e-mails and supporting documentation which is on file with the ISRM Office.

The Agency Risk Management and Internal Control Standards (ARMICS) team evaluates VDSS internal controls and makes recommendations for improvements. This team also acts as a consultant to VDSS

division/directorate/office/district/regions and LDSSs interested in establishing internal controls. The ARMICS reports summarize the activities of the ARMICS team regarding transaction-level assessments of internal controls for VDSS key fiscal processes. A report for each fiscal process is produced and includes the control activities that were identified and tested, effectiveness of controls, recommendations, and the status of CAs.

In determining the overall risk for VDSS, an enterprise-wide RA tool is used. The current tool examines approximately 200 processes and relative risk is measured across 14 factors such as level of federal funding received, **confidentiality** of information, and complexity of operations. A weighted rank order of the processes based on risk is then produced which provides overall direction, which VDSS, the ARMICS team, and Continuity Planning (CP) efforts (including BIAs) use to focus their attention.

This program and related standards are based on protecting VDSS systems and data based on **sensitivity** and risk, including system **availability** needs. Accordingly, RM is a central component of the **VDSS Information Security Program** and allows VDSS to determine how these factors apply to its information systems.

VDSS started the RM process with a BIA. A BIA is a process of analyzing VDSS business functions, to identify those that are essential or those that contain **sensitive** data, and assessing the resources that support them including information systems. For the purposes of information security, the BIA identifies those business functions that are essential and that are dependent on IT. This analysis is necessary in order to determine the appropriate level of protection for information systems and the data they process.

After appropriate mitigating information security controls have been applied relative to **sensitivity** and risk, based on the RA results, **sensitive** IT systems require periodic, independent *IT Security Audits*. These audits are necessary to determine whether the overall protection of IT systems and the data they handle is adequate and effective.

IT Security Audits may identify additional mitigating controls for **sensitive** IT systems in order to provide adequate and effective protection of the systems and the data they handle. After applying these controls, the final step in the RM process is formal acceptance by the Commissioner or designee of any residual risk to VDSS operations from **sensitive** IT systems.

Related References:

[Government Data Collection & Dissemination Practices Act \(GDCDPA\)](#)

[VDSS Nondisclosure Agreement \(.pdf\)](#)

4.1.1 Sensitive Data Definition

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** - This addresses *sensitivity* to unauthorized disclosure.

Examples include:

- 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;
- Workers querying Application Benefit Delivery Automation Project (ADAPT) to determine a family member's status of a benefits application; 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** - This addresses *sensitivity* to unauthorized modification.

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** - This addresses *sensitivity* to outages, such as those determined by the BIAs.

Examples include:

- VDSS e-mail system will not be **available** in a disaster if the e-mail provider is rendered inoperative and the e-mail 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 division/directorate/office/district/regions and LDSS.

The following information/data is considered "**Sensitive** Information":

- Third-party **confidential** information (both sent and received);
- PII (anything that could be used to identify a specific person) as covered by the GDCDPA;
- Federal Tax Information (FTI) information that originated from the Internal Revenue Service (IRS), Social Security Administration (SSA), or Department of Labor.

- Financial information as protected by the Payment Card Industry (PCI) Security Standard; or when *integrity, confidentiality, and/or availability* are an issue; and
- Commissioner's working papers or correspondence 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.

If in doubt about a non-disclosure issue, contact the VDSS CISO to determine the appropriate security level and whether a non-disclosure agreement is required. If there are concerns and potential legal issues, the VDSS CISO should contact legal counsel for further interpretation before action is taken. This step will avoid a potential interruption in VDSS business.

4.1.2 Business Impact Analysis

A critical component of any business continuity program is the conduction of a BIA. A BIA is a process designed to prioritize business functions by assessing their potential quantitative (financial) and qualitative (non-financial) impact that might result if VDSS experiences a business continuity event (i.e., an interruption of significant duration). BIAs provide the foundation to any viable business continuity program.

The result of the BIA for VDSS will be a prioritized list of major business functions along with a strategy to sustain, or recover from, any type of disruption. Other benefits are identification of any known or potential risks, which will be fed into subsequent RAs. All information gathered is used to revise VDSS Continuity Plans.

4.1.3 Risk Assessment (RA)

Based on the results of the BIA; specifically, impact rating and Recovery Time Objective (RTO), RAs will be conducted for all VDSS-owned critical information systems classified as *sensitive*. RAs delineate the steps VDSS must take for each IT system classified as *sensitive* to:

- Identify potential threats to the IT system and the environment in which it operates;
- Determine the likelihood that identified threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

This is achieved by:

- Identifying IT systems that contain *sensitive* information and, thus, require ongoing RA reviews;

- Examining IT system documentation, especially security measures included in its design;
- Examining access controls in place to protect *sensitive* data;
- Collecting information via interview and questionnaires regarding *confidentiality, integrity, and availability* controls in place versus what is deemed to be needed; and
- Writing a RA report for management review that includes findings and recommendations to mitigate identified risks and vulnerabilities.

4.1.4 Security Audits

As required by COV in the *IT Security Audit Standard*, VDSS is to conduct IT security audits of systems and government databases which contain *sensitive* information. For security purposes, the ISRM Office must also ensure that federally-sourced data is appropriately secured and controlled. In this section, *sensitive* information also includes data which is federally-sourced.

The protection of VDSS-held data is also, in some cases, prescribed by law. Client information gathered and used for purposes of administering programs and providing services, in many situations, can only be used for those purposes and the information cannot be distributed or shared for any other purpose either inside or outside of VDSS and LDSS.

If *sensitive* systems contain federal data, such as that received from the IRS and the Social Security Administration (SSA), there are additional protections which must be in place and functioning to meet federal requirements. One example of the protections around federally-sourced data prescribes that all worker views of Federal Tax Information (FTI) via VDSS systems must be logged and the logs retained for 6 years.

A three-year IT Security Audit Plan is developed and executed which covers all systems which contain *sensitive* information. Audit reports are issued and follow-up actions are performed relative to the outstanding findings identified during the audits.

4.2 Continuity Planning (CP)

CP defines business processes and all necessary supporting items, such as information systems/applications/data, that are needed if an event occurs that renders VDSS unable to operate.

CP includes:

- Emergency Response Plans
- Business Continuity Plans
- IT Disaster Recovery (ITDR) Plans
- IT System and Data Backup and Restoration Plans

The results of CP are the Agency Continuity Plan and Division-level Continuity Plans. The VDSS Continuity Plan is mandated by the Virginia Department of Emergency Management (VDEM) and must

be submitted to them annually, using the official COV template, by April 1st of each year.

4.2.1 Emergency Response Plans

The VDSS Emergency Response Plan is in development and coordinated by the VDSS Offices of General Services and Emergency Management within DOF. It will include information such as evacuation procedures, first aid/cardiopulmonary resuscitation (CPR), and shelter-in-place, etc. (i.e., all information needed for the first hours following any type of disruption).

4.2.2 Business CP

All executive Agencies within the COV are required to submit Continuity Plans to VDEM annually no later than April 1st. This requirement is supported by Executive Order (EO) #41 (2011) entitled “Continuing Preparedness Initiatives in State Government and Affirmation of the Commonwealth of Virginia Emergency Operations Plan.”

Business Continuity Plans are activated during or immediately after the Emergency Response Plans are in use. Per requirements by VDEM, the VDSS Continuity Plan contains VDSS Mission Essential Functions (MEFs) and Primary Business Functions (PBFs) that support the MEFs. It also includes details for how, when, why, where, and by whom the MEFs and PBFs will be recovered in a disaster situation. VDSS has a Recovery Leadership Team (RLT) that will direct the recovery efforts until the primary facility (or a new one) is available for occupancy.

Essential VDSS business functions are identified by the completion of a BIA (described above). These functions may or may not be dependent upon IT resources.

In addition to the VDSS Continuity Plan, each Division within VDSS has its own Continuity Plan that mirrors the VDSS plan and further describes how each division will respond to an emergency and recover their business functions.

4.2.3 IT Disaster Recovery (ITDR) Plans

ITDR planning is required by COV in the *IT Information Security Policy*. ITDR planning supports CP by defining specific policies, standards, procedures, and processes for restoring IT systems and data that support mission essential business functions on a schedule that supports the Agency’s mission requirements. Based on identified RTOs and Recovery Point Objectives (RPOs), the IT system backup and restoration plan ensures that IT systems/applications/data can be recovered as required.

The VDSS Division of Information Systems (DIS) is responsible for creating and maintaining the VDSS ITDR plan, working in conjunction with the ISRM Business Continuity Manager to sync recovery of information systems to priorities established in the BIA to accommodate RTOs and RPOs. DIS works closely with VITA/NG to accomplish ITDR planning.

¹ RTO (Recovery Time Objective): The period of time within which systems, applications, or business functions must be recovered after an outage, enumerated in business time (e.g., within one business day) or elapsed time (e.g., within 48-72 hours).

² RPO (Recovery Point Objective): Identifies the amount of data loss that can be tolerated (e.g., two hours) that dictates how often the data must be backed up.

4.2.4 IT System and Data Backup and Restoration Plans

IT system and data backup and restoration plans are components of the ITDR plan and, thus, the responsibility of the VDSS DIS. These plans must be implemented to create a comprehensive backup plan, including standards and operational procedures, executed during a system backup. The plans correspond to the needs identified in the BIA. These plans include standards and operational procedures to be executed during system restoration. The information in these plans must directly correspond to agreements between VDSS and VITA/NG for backup and recovery services.

Related References:

[COV IT Information Security Policy](#)

[COV Information Security Standard \(.pdf\)](#)

[COV IT Risk Management Guideline \(.pdf\)](#)

[COV IT Risk Assessment Guideline, Appendix D – Risk Assessment Instructions \(.pdf\)](#)

[COV Risk Assessment Report Template \(.doc\)](#)

[Executive Order #41](#)

[VDEM Continuity Plan Template \(.doc\)](#)

[COV IT Contingency Planning Guideline \(.pdf\)](#)

4.3 Information System Security Plans

An Information System Security Plan (ISSP) must document the security controls in place to protect information systems against security risks as identified during a Risk Assessment.

Related References:

Information System Security Plan – Prepared by VDSS/DIS for VDH/IS in regard to the Adult Services/Adult Protective Services (ASAPS) System, approved April 8, 2011

4.4 Information Systems Interoperability Security

The systems that can be accessed through Systems Partnering in a Demographic Repository (SPIDeR) are on a variety of technical platforms. Some of these systems belong to VDSS and some belong to the IRS, the SSA, the Virginia Employment Commission (VEC), the Division of Motor Vehicles (DMV) and others.

For LDSS staff, authorization to the SPIDeR system is determined and approved by the LDSS Director. All VDSS staff members need authorization from their Director. In both cases, access will only be

approved if it is necessary to fulfill job responsibilities. All state and federal *confidentiality* rules apply when accessing the data.

4.5 IT System Application Security

Application security controls are in place to define the high level specifications for system applications for VDSS. During application planning data is classified according to the *sensitivity* of the data. A RA is conducted before development begins and after planning is complete, if the data classification identifies the system as *sensitive*. Early in the development lifecycle, security requirements of the application are identified and documented. The results of the Data Classification process are used to assess and finalize any encryption, authentication, access control, and logging requirements. Please refer to DSS Applications Development requirements Policy, prepared 3/11/2011, developed by the ISRM Office for specific application development, production and maintenance security requirements. All VDSS system development efforts (either new systems or significant modifications to existing systems) must involve the VDSS ISRM Office in all phases of system development.

Usage of VDSS systems is logged. This logging enables the VDSS ISRM Office to determine who did what, to what record, and when it was done. Viewing of FTI is also logged.

Related References:

[Applications at VDSS](#)

[DSS Applications Development Requirements Policy](#) (.docx), DOF, ISRM Office, March 1, 2011

4.6 Remote Access

VDSS uses the NG provided Cisco's virtual private network (VPN) client for remote access. The specific level of VPN security access requirements will be determined based on the system you are accessing.

4.6.1 Single-factor authentication (SFA)

Single-factor authentication (SFA) is the traditional security process that requires a user name and password before granting access to the user. Single Factor VPN is part of the standard image deployed on all VDSS laptops. All State and Local workers have SFA created at the time as your COV Domain account is created. This is the account you log on to your computer with each day. Contractors do not automatically have a SFA created and one must be requested depending on the requirements of each particular Vendors Contract.

4.6.2 Dual-factor authentication (DFA)

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a key fob, and the other of which is typically something memorized, such as a key fob PIN number. An access request process has been developed for the Dual Factor Token. The Dual Factor Token form is sent as an attachment to the VDSS ISRM

Office at security@dss.virginia.gov and will normally be submitted/approved by the ISO, Manager or Director. Additional requirements include **business justification**, what applications will be accessed and whether the token will be used for telecommuting. The security token and instructions will be provided to the employee or the approver. These tokens cost approximately \$150 each and should only be requested to meet **business needs**, and not as a matter of convenience. Periodically, utilization reports are requested to ensure security tokens are being used where needed most.

4.6.3 Password Requirements for Dual Factor Token PIN

- Choose a PIN with a minimum length of **seven alphanumeric characters**
- Change the PIN every **90 days**

Note: The IRS expressly prohibits the use of privately owned equipment to access data systems containing IRS-provided data.

Note: Only COV equipment can be used to connect to the Agency network or to store Agency data. The use of personal thumb drives is expressly prohibited.

Related References:

[DSS VPN Verification Instructions](#) (.pdf)

[Dual Factor Token](#) (.docx)

[VDSS Acceptable Use Policy](#) (.pdf)

[VPN Site-to-Site Change](#) (.doc)

4.7 Wireless Security

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. VDSS employees can use a variety of wireless access systems, and the most frequently used are discussed in the following sections. Any access not specifically addressed below is prohibited unless explicit permission is granted from the VDSS ISRM Office.

4.7.1 Guest Wireless

VDSS Home Office has recently added the capability to provide Visitors of VDSS Guest Internet access in the all main conference rooms. This will provide Internet access only and not serve as a connection path to VDSS systems or to the COV network. A request for Visitors' access to the Wireless Guest Network must be submitted by the VDSS sponsor of the visit who can affirm the Visitor's business need for access. To ensure that access is established by the time of the Visitor's arrival, please plan ahead and allow 3 to 5 business days for establishing the account and delivery of user id, password and instructions.

The responsible sponsor should complete the **Guest Wireless Internet Access Request** and send the completed form electronically to (guest.wireless@dss.virginia.gov). When the ISRM Office grants

access, they will e-mail the Visitor the “Guest User Details” to the e-mail account included on the access request. This e-mail will provide the Username and Password, the Terms of Use, and the instructions for logging into the wireless network. Included in the Terms of Use will be the statement “by using this account I agree to abide by Terms of Use as provided.”

Note: Other use of wireless communication is prohibited without express written consent from the VDSS CISO.

Related Reference:

[Guest Wireless Internet Access Request \(.pdf\)](#)

4.7.2 Wireless for VDSS systems

Due to the *sensitivity* of much of the information that VDSS/LDSS uses, very strict controls are required. A two-factor authentication (addressed in Section 4.6.2) is required to access any Agency system which contains sensitive data that is covered under Federal Rules.

COV has selected the RSA token as the primary source for this second layer of authentication. See Section 4.6.2 for information on these tokens.

The following systems require a Dual Factor Token for remote access due to the *sensitivity* of the data:

1. ADAPT
2. SPIDeR
3. VaCMS
4. MWS
5. APECS
6. SVES

The following systems require a Dual Factor Token due to the configuration of the COV Domain.

1. LETS
2. FAAS
3. LASER
4. Most Server Administrative Functions
5. ClearQuest

4.7.3 Wireless from Home or other Public Places

VDSS users need to ensure, when accessing external wireless connections, that the session is encrypted and appropriately secured. Use of the VPN client or dual factor token provides this assurance. Without using these tools, the user must access web sites using SSL or https. Using personal equipment to access VDSS systems from home is prohibited on privately owned equipment. The only exception is to access Webmail.

4.7.4 Wireless in Local Offices

Wireless in local offices must comply with the same requirements as those deployed by VDSS. Any exceptions must be coordinated through the CISO and permissions explicitly granted. Specific Wireless requirements are listed in COV Security Standard SEC 501-06. Before you add wireless access to any system you should submit the plan for implementing this capability to the CISO for review and approval before any funds are expended.

4.8 Mobile Devices

According to the *VDSS Acceptable Use Policy*, users may access their COV-provided e-mail from any personal computer, smart phone, I-Pad, or other devices, using the Internet. Users who remotely access any *other VDSS resources will use only VDSS-provided equipment* that is configured, set up and maintained by VITA/NG technicians without modification or similar equipment provided by a locality that is not supported by the Commonwealth's partnership with NG. At a minimum the selection, implementation and use of mobile devices must include the elements outlined the COV Mobile Device Security Policy. Mobile Devices purchased and owned by Local Governments to support LDSS operations are covered under this same approval as long as they subscribe to the same mobile device manage as the VDSS provided equipment.

Good for Enterprise™ has been selected for mobile device management in the COV and VDSS. The secure mobile device management (MDM) solution and collaboration suite, Good for Enterprise™ is designed to reduce data loss on today's most popular iOS, Android, and Windows Phone mobile devices. All LDSS that use I-PADs to access COV networks or applications need to use Good for Enterprise™ purchased through VITA or procured by your local government. This service should be ordered at the time of purchase or as an additional service to existing devices thru the current equipment management process managed by the DSS IT Services Manager. A standard feature of this service is the ability to remotely wipe data from devices if they are lost or stolen. To subscribe to the service you must:

Open a ticket with the VCCC and have it assigned to the DSS-IT SERVICES MANAGER group requesting a Work Request be submitted for ENTERPRISE HANDHELD SERVICES (NON-BLACKBERRY).

*Note: The use of non-COV owned mobile devices is **expressly prohibited** to access VDSS applications and networks. The only authorized use of personally owned devices is to access Webmail.*

Related Reference:

[COV Mobile Device Security Policy \(.pdf\)](#)

[Good for Enterprise™](#)

4.9 Logical Access Control

Logical Access Control requirements define the steps necessary to protect the *confidentiality, integrity, and availability* of VDSS systems and data against compromise. Logical Access Control requirements identify the measures needed to verify that all IT system users are who they say they are and that they are

permitted to use the systems and data they are attempting to access. Logical Access Control defines requirements in the areas of Account Management, Password Management, and Remote Access.

The principle of *Least Privilege* must be followed for all employees who access VDSS systems.

A basic principle in information security, *Least Privilege*, holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

Note: *No one* can approve/implement access changes for themselves. In the case of a SO updating SAMS another SO must make the access changes. SAMS was updated in 2012 to prevent a SO from changing their own access.

4.9.1 Account Management

Account Management standards and procedures must be implemented to ensure the steps necessary for requesting, granting, administering, and terminating accounts at VDSS are formalized. **ALL** Access Request Forms **must** be submitted electronically. Access request forms are located on the SPARK web site under Forms on the ISRM section.

4.9.1.1 Non-Paid Employees

The LDSS Office should consider its (volunteers, student interns, and various community organizations) as Non-Paid Employees to comply with Federal, and State code restrictions on use/disclosure requirements if their local legal representative has approved the use of Non-Paid Employees. Note: This designation as a Non-Paid Employee is only for data security/access purposes and is not intended to confer the rights that paid employees have, such as access to the grievance system or other benefits.

If the LDSS Office has approval to use Non-Paid Employees they also need to develop a Local Confidentiality/Non-Disclosure Agreement for the Non-Paid Employee to sign. This agreement must also be reviewed and approved by the local legal counsel. The agreement should include:

- a. Statement of understanding the nature of the information they are being granted access to;
- b. The limits of its use; and
- c. Understanding of the legal penalties that unauthorized use and/or disclosure can result in.

The LDSS Office should retain this document together with the VDSS Acknowledgement of Acceptable Use and all access requests to comply with standard retention schedules.

4.9.1.2 Seasonal Worker

Seasonal workers with up to 90-days between work dates - No special requirements.

Seasonal worker with 90 to 179 days between work dates – Requires an e-mail to reset the account; the e-mail must come from the person(s) who approved the original access request.

Seasonal worker with 180 days or more between work dates – Should be terminated. Must submit new request forms for access.

In all cases, the SO should suspend the seasonal worker's account any time they will be gone for more than 30 work days.

4.9.1.3 Approval Process Flow for VDSS Security Forms

1. The Worker (or the Supervisor) fills out the form and e-mails it to the Supervisor.
2. The Supervisor approves and forwards via e-mail as noted on each Access Request form instructions. (*NOTE: Some access requires the Director to approve, while most only require the supervisor.*)

Approval Checklist

- ✓ Verify the e-mail came from the employee.
 - ✓ Give the **business justification** for the access requested by the worker:
Example: Employee is a Benefit Program policy trainer and needs to train on both ADAPT and the program policies that use the ADAPT system.
 - ✓ Form is renamed: Example: ADAPT-LOCAL-Doe John.doc
 - ✓ The Supervisor types in their name and the date on the form, saves it, and e-mails the form as appropriate to the routing on the particular form. *Please see the **Access Request Form** for specific instructions.* A description subject line in the e-mail should be included:
e.g., ADAPT Access Request – FirstName LastName
3. Approves and forwards via e-mail to the Local SO.

Director Approval Checklist

- ✓ Verify the e-mail came from supervisor.
 - ✓ Verify the form has **business justification** or the access requested by the worker.
 - ✓ The Director types in their name and the date on the form and e-mails the form to the Local SO.
4. The Local SO reviews and sends via e-mail to security@dss.virginia.gov.

Local SO Checklist

- ✓ Ensure that the form is completely filled out.
- ✓ Verify the **business justification** has been completed.

- ✓ Ensure that the e-mail chain shows e-mails sent from the supervisor (to the director, if required) and to the Local SO with all names showing on the form.
 - ✓ The Local SO saves the official Local copy of the access form (suggest electronically).
 - ✓ The Local SO creates the access unless it is a contractor or unless instructed to do otherwise in the form's instructions.
5. The VDSS ISRM Office reviews and processes all properly documented and approved access requests.

*Note: The Director **must approve** SO changes, requests for local administrative rights, SPIDeR access requests, or firewall changes.*

Related reference:

[Access Request Forms on SPARK](#)

4.9.2 Password Management

Passwords are used in many ways to protect data, systems, and networks. For example, passwords are used to authenticate users of operating systems and applications such as e-mail, labor recording, and remote access. Passwords are also used to protect files and other stored information, such as password-protecting a single compressed file, a cryptographic key, or an encrypted hard drive. VDSS uses the Open Lightweight Directory Access Protocol (LDAP), an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

Effective password management reduces the risk of compromise of password-based authentication systems. VDSS needs to protect the **confidentiality**, **integrity**, and **availability** of passwords so that all authorized users—and no unauthorized users—can use passwords successfully as needed. **Integrity** and **availability** should be ensured by typical data security controls, such as using access control lists to prevent attackers from overwriting passwords and having secured backups of password files. Ensuring the **confidentiality** of passwords is considerably more challenging and involves a number of security controls along with decisions involving the characteristics of the passwords themselves. For example, requiring that passwords be long and complex makes it less likely that attackers will guess or crack them, but it also makes the passwords harder for users to remember, and thus more likely to be stored insecurely. This increases the likelihood that users will store their passwords insecurely and expose them to attackers.

VDSS has adopted **strong password** criteria. A **strong password**:

- Is at least eight (8) characters.
- Does not contain the user names, a real name, or VDSS.
- Does not contain a dictionary word.

- Is significantly different from previous passwords.
- Contains uppercase and lowercase letters and alphanumeric characters.
- Contains sixteen characters maximum.
- Cannot be reused except after 24 times using other passwords.

4.10 Data Protection

Data Protection provides security safeguards for the processing and storing of data. This component of the **VDSS Information Security Program** outlines the methods that can use to safeguard the data in a manner commensurate with the *sensitivity* and risk of the data stored. Data Protection includes requirements in the areas of Media Protection and Encryption. VDSS has seven main systems that store and/or capture *confidential* information that users must safeguard against unauthorized disclosure and access.

These systems are:

- OASIS
- ADAPT
- APECS
- SPIDeR
- VaCMS
- EDS-CP

OASIS (Online Automated Services Information System) is an online case record system related to Family Services cases. Family Services promotes and supports the development of healthy families and helps protect Virginia's children and adults from abuse and neglect. OASIS:

- Contains information relating to Child Protective Services, Foster Care and Adoption and is the system of record for these areas; and
- Contains some of the most sensitive and restricted data for use by VDSS/LDSS employees.

OASIS is also a primary source of data for federal, state and local child welfare Agencies' reporting and planning efforts. Currently, OASIS contains information relating to Child Protective Services, Foster Care and Adoption.

ADAPT (Application Benefit Delivery Automation Project) is used by the Division of Family Services (DFS) to provide an online case record, available statewide to authorized LDSS and home office users, of information related to Family Services cases.

APECS (Automated Program to Enforce Child Support) is the statewide automated system that supports the Commonwealth's child support enforcement program. APECS combines all types of child support cases within one integrated system, and it features both case management and financial management capabilities. It is certified by the federal Office of Child Support Enforcement (OCSE) as meeting all requirements mandated by the Family Support Act of 1988 and the Personal Responsibility and Work Opportunity Reconciliation Act of 1996.

SPIDeR (Systems Partnering in a Demographic Repository) is a system which not only acts as a repository for various VDSS publishing systems, but also provides access to other state and several federal Agencies' citizen-level information. SPIDeR also publishes client-level information to various VDSS systems either from the repository and it also reaches back to other systems and pushes data to recipient systems. Because of the data SPIDeR receives and handles, SPIDeR is considered a sensitive system which also contains federally-sourced data.

SPIDeR also provides pathways for users to directly inquire other COV Agency information (such as that information available from DMV and VEC), as well as certain federal systems (such as SSA's SOLQ-I (SSA State Online Query)).

SPIDeR contains audit logging capabilities which capture all users' actions conducted within or through SPIDeR. The ISRM Office can pull audit logs for all SPIDeR users' activities and uses the audit logs to provide assurances regarding the access to and use of SPIDeR information by employees.

Access to SPIDeR is restricted to VDSS/LDSS employees only. No contractors, volunteers, or other non-employees should have access to or use of SPIDeR due to the sensitive and federally-sourced information contained within SPIDeR. There are no provisions made within the various LDSS MOAs which allow contractors, volunteers, or other non-employees to access or use SPIDeR.

Systems Currently Partnered with SPIDeR:

- ADAPT (Application Benefit Delivery Automation Project)
- APECS (Automated Program for the Enforcement of Child Support)
- ASAPS (Adult Services and Adult Protective Services)
- COOL
- DMV (Department of Motor Vehicles)
- EDSP-CP (Enterprise Delivery System Program Customer Portal)
- FUEL (Heat/Cool)
- OASIS (Online Automated Services Information System)
- SDX (State Data Exchange)
- SOLQ-I (SSA State Online Query)
- SVES/SOLQ
- MEDPEND (Medicaid Pending)
- VACIS (Virginia Client Information System)
- VaCMS (Virginia Case Management System)
- VaMMIS (Virginia Medicaid Management Information System)
- VEC (Virginia Employment Commission)
- Work Number (third-party employment information provided by TALX Corporation)

VaCMS (Virginia Case Management System) automates the Child Care program for the Division of Child Care & Early Childhood Development in VDSS.

EDSP – CP (Enterprise Delivery System Program - Customer Portal) provides VDSS customers and employees access to unified benefits, child care applications and reporting.

4.10.1 ISRM Safeguards Program (SP)

The ISRM Safeguards Program (SP) was implemented in June 2011 to ensure that VDSS has uniform safeguard standards for protecting FTI. The safeguard review is an onsite evaluation of the use of FTI and the measures employed by the Division of Benefit Programs, each District Division of Child Support Enforcement (DCSE) and LDSS office to protect the data. The Safeguard Review Team will conduct the review to ensure that VDSS is in compliance with the IRS, SSA, COV, and VDSS minimum protection standards for protecting FTI data.

The following key elements will be reviewed during the Safeguard inspections:

- a) employee awareness;
- b) record keeping;
- c) secure storage;
- d) limited access;
- e) disposal; and
- f) computer systems security.

Reviews of DCSE offices will be conducted once every two years unless otherwise noted by the reviewer, and reviews of LDSS offices will be conducted once every three years unless otherwise noted by the reviewer.

The Safeguard Review Team will work together with DCSE and LDSS offices to provide assistance with how to better protect clients' *confidential* FTI data.

Related References:

[IRS Publication 1075 \(.pdf\)](#)

[Social Security Program Rules](#)

4.10.2 Data Storage Media Protection

Data Storage Media Protection identifies the steps required for the appropriate handling of stored data to protect VDSS data from compromise. *Sensitive* data may not be stored on mobile data storage media, including laptops as well as any non-network drive, except for backup media, unless the data is encrypted and there is a written exception approved by the Commissioner. Logical and physical protection is required for all data storage media containing *sensitive* data, commensurate with *sensitivity* and risk.

Storing any data classified as *sensitive* on any mobile device including laptops and any non-network drive, but excluding backup media, is prohibited unless the data is encrypted and there is a written exception approved by the Commissioner or designee identifying the business case, risks, mitigating logical and physical controls, and any residual risk.

A vendor, who stores *sensitive* information (as defined by VDSS) on their system, must keep that data *confidential*, and destroy information after it is no longer necessary. Vendors should sign a *Non-Disclosure Agreement* to ensure that this is part of the contract.

4.10.3 Encryption

VDSS no longer has a private network. All communications to and from state and local social service workers is now transmitted through the Commonwealth's enterprise network along with communications to and from many other state Agencies.

In order to protect the *confidentiality* of *sensitive* information (e.g., PII) transmitted in electronic communications, it is now necessary to encrypt the *sensitive* information prior to transmission.

VDSS uses Microsoft File Encryption to encrypt *sensitive* information that will be sent over the Internet.

Note: VDSS allows the use of encrypted USB drives as long as the worker's supervisor has the password to the device. This process is required to ensure VDSS can access the data if the worker leaves. This exception to COV policy has been signed by the VDSS Commissioner.

Related References:

[Encrypting – E-mail \(.pdf\)](#)

[Encrypting – Word \(.doc\)](#)

4.11 Facilities Security

Facilities Security safeguards require planning and application of facilities security practices to provide a first line of defense for IT systems against damage, theft, unauthorized disclosure of data, loss of control over system *integrity*, and interruption to computer services. For example, access to the VDSS computer facility is restricted to those individuals listed on the VDSS Computer Room Access List. Any individual not appearing on the list must be logged in and escorted by a VITA/NG employee. Furthermore, Sonitrol swipe cards protect the VDSS computer facility against physical access by unauthorized personnel. Physical access to essential computer hardware, wiring, displays, and networks is only provided to those individuals who need it to do their jobs.

*Security Tip: Protecting FTI is everyone's responsibility. To prevent unauthorized access to **confidential** FTI data, verify the identity of all visitors/unauthorized individuals and have an authorized employee escort them while in a restricted area of your building.*

Related Reference:

Physical Security for Employees, Visitors and Property at Home Office – January 2006

4.12 Personnel Security

Personnel Security controls reduce risk to VDSS systems and data by specifying Access Determination and Control requirements that restrict access to these systems and data to those individuals who require such access as part of their job duties. Personnel Security also includes SATP requirements to provide all IT system users with appropriate understanding regarding the VDSS ISPs and the **VDSS Acceptable Use Policy** requirements for VDSS systems and data.

4.13 Logical Access Determination and Control

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied. Personnel security safeguards take into account 1) granting or withdrawing physical and system access privileges upon: hiring an employee, updating access, transferring an employee to another VDSS entity or state Agency, terminating an employee, or when an employee resigns or changes job duties within a VDSS entity; 2) system access will be granted via a formal and auditable process, 3) security training will be conducted within 30 days of a new hire, 4) **Non-Disclosure Agreements** will be signed by all individuals who need access to "**sensitive**" information, prior to granting access to that information, 5) Background checks of personnel may be required consistent with VDSS entity policy and depending on the **sensitivity** of information accessible to that position.

Security Access Management System (SAMS) was conceived to provide a platform for the ISRM Office to grant, update, delete access and validate access granted to VDSS systems users and addresses the Auditor of Public Accounts (APA) Audit Report recommendations and findings delivered in December 2005.

LDAP is the system of record for VDSS which keeps a record of employees profile and the systems they have access to. Since SAMS matches the employees profile and the systems access privileges to the HR and VDSS systems and provides exception reports to the ISRM Office, any new system that needs to be brought in to the match process needs modifications to the LDAP administration tool as well.

Related Reference:

Approval Process Flow for DSS Security Forms – Section 4.4a Account Management

4.14 Third-Party/Contractor Requirements

The **Third-Party Non-Disclosure Agreement** will be used when a contractor will be given access to sensitive IT systems and/or data for which there is a risk associated with data disclosure. The contractor shall take all precautions and measures necessary to ensure the **integrity**, non-disclosure, **confidentiality** and protection of all data and information obtained from VDSS including, but not limited to all original reporting forms and data in any other form.

Contractors who, for example, are asked to enter data into VDSS systems including the Virginia Case Management System (VACMS) are specifically required to:

1. Adhere to the **VDSS Acceptable Use Policy** dated June 10, 2011;

2. Adhere to the *COV Information Security Standard* dated April 4, 2011; and
3. Complete documents including the *VDSS Computer Access Request Form*, *Non-Disclosure Agreement*, and *Agency Request for Token (Reassignment)* and any other system access forms as necessary.

Furthermore, the *contractor's Agency* is responsible for the following *System Security Requirements*:

1. A criminal background check is conducted on all employees who will be issued a Userid to access VDSS systems;
2. Access request documentation must be submitted to the proper VDSS SOs in the prescribed format and means;
3. Ensure all employees complete and attest to the completion of the required training prior to requesting access, (i.e., *Acceptable Use Policy* and *COV Information Security Standard*), and the *Non-Disclosure Agreement*;
4. On last day of employment or last day access is required, proper VDSS SOs must be notified on the provided access form of termination of employment/access and return/mail the Dual Factor Token to VDSS Information Security and Risk Management Office, 801 East Main Street, 15th Floor, Richmond, Virginia 23219;
5. Pay to replace any Dual Factor Tokens that are damaged or lost by employees. Cost will be based on replacement cost at time of purchase; and
6. Prohibit the downloading or copying of any information contained in VDSS systems to any other computer system or computer application.

Employees who require access to the COV's network and VDSS systems must abide by the following conditions:

1. Read and comply with the *VDSS Information Security Program* requirements provided by VDSS SOs including updates and revisions;
2. Read and sign a *Non-Disclosure Agreement* before being granted access to VDSS systems;
3. Read and sign the *VDSS Acceptable Use Policy* form to indicate the reading and acknowledgement of VDSS security policies and procedures;
4. Annually complete the SATP via the COV Knowledge Center;
5. May not use COV-provided network access credentials from any location other than the business address for the contractor and affiliates listed, especially not from home or any public access systems such as a public library, school, or commercial hot spot;
6. Protect and properly use the Dual Factor Token provided to access VDSS system(s). Use of the token is restricted to the individual to whom the token was issued;
7. Report a lost/missing Dual Factor Token within 24 hours of discovery to the VDSS CISO (security@dss.virginia.gov) or (804) 726-7891; and

8. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

4.14.1 Equipment and Software Ownership

Contractors and/or affiliates must:

1. Own all equipment (computers, printers, network and storage devices) that are connected to the COV's network and used to access VDSS systems;
2. Purchase and install a CISCO VPN Software solution;
3. Purchase and install an Anti Virus Product and provide proof of current Anti Virus Product upon request; and
4. Own all software including Internet Explorer used to access VDSS systems.

4.14.2 Reporting

The *contracting Agency* will report annually on the contract renewal date or upon change to any of the following items submit to the proper VDSS ISO:

1. Complete list of all equipment to include manufacturer, model, and serial number;
2. Proof of Purchase or certification of Anti-Virus Program for each computer in item 1 above;
3. Proof of Purchase for all software related to the VDSS project loaded on the computers in item 1 above;
4. List of current employees working under the authority of this contract and the address from which staff will be working and accessing the COV network and the VDSS application; and
5. Copy of a written contract that binds the listed affiliate Agencies to the requirements of this contract.

4.14.3 Incident Reporting

1. Any suspected or inappropriate access or suspected improper updating of information must be reported to the VDSS CISO (security@dss.virginia.gov) or (804) 726-7915 within 16 hours of discovery; and

The report shall include:

- a. Name of person making the report;

- b. Contact information to include telephone number, e-mail and mailing address;
and
 - c. Brief description of the incident.
2. Information requested by the VDSS CISO relating to incidents or employee access issues must be provided within 48 hours of request in a *written* form.

Notes:

- *No one outside VDSS will get server administrative rights.*
- *VDSS must identify all contractors with access to FTI and the purpose for which access was granted.*

Related References:

2011 SAR security access review document – Item 7.4.5

[VDSS Nondisclosure Agreement](#) (.pdf)

[Incident Management and Internet/EAL/SPIDeR Request Flowchart](#) (.xlsx)

[Incident Management and Internet/EAL/SPIDeR Request Reporting Procedure](#) (.doc)

4.15 Security Awareness Training Program (SATP)

SATP focuses on identifying risks, threats, and vulnerabilities of VDSS information systems and how to fix them.

Topics covered in security awareness training include:

- The nature of *sensitive* material and physical assets encountered during routine business;
- Employee and contractor responsibilities in handling *sensitive* information, including review of employee nondisclosure agreements;
- Requirements for proper handling of *sensitive* material, including marking, transmission, storage and destruction;
- Proper methods for protecting *sensitive* information on computer systems, including password policy and use of two-factor authentication;
- Other computer security concerns including malware, phishing, social engineering, etc.
- Workplace security including building access, wearing of security badges, reporting of incidents, forbidden articles, etc.; and

- Consequences of failure to protect information, including potential loss of employment, economic consequences to VDSS and the COV, damage to individuals whose private records are divulged, and possible civil and criminal penalties.

The VDSS ISRM Office has developed several methods of accomplishing its SATP objectives:

- **New Employee Orientation.** Present security training to all new employees during the New Employee Orientation (NEO) sessions given by the Division of Human Resources (DHR);
- **Information Security Program.** Supply each employee with a copy of the *VDSS Information Security Program*; and
- **E-mails and Broadcasts.** Inform individuals of security concerns, issues and warnings using various electronic communication formats such as direct e-mails and SPARK Broadcast messages.

4.16 Acceptable Use

VDSS provides computers and computer accounts to its staff to assist them in the performance of their jobs. The computer systems and networks belong to VDSS, and the user may use the system for authorized purposes only. The *VDSS Acceptable Use Policy* is an integral part of the framework of ISPs. New employees and contractors of the VDSS are required to sign the *VDSS Acceptable Use Awareness Acknowledgement* before access to information systems and data is granted. Acceptable use of the Internet consists of activities necessary to support the purpose, goals, and mission of VDSS division/directorate/office/district/regions and LDSS and each user's authorized job functions as expressed in the Employee Work Profile (EWP).

Personal use of the Internet is permitted during:

- Established lunch periods – Usage must be less than 15 minutes in any continuous hour;
- Break periods – Usage must be less than 5 minutes; and
- Before and after established work schedule – Less than 15 minutes in any continuous hour.

Use of personally-owned equipment such as scanners, Universal Serial Bus (USB) thumb drives, smart phones and computers to store and/ or process information *that has been determined to be sensitive* during a RA or BIA is strictly prohibited and not allowed by COV Standards.

Compliance with the *VDSS Acceptable Use Policy* is measured by regular audits.

Related References:

[Acceptable Use \(06-10-2011\)](#) (.pdf)

[Information Security Program & Acceptable Use Awareness Acknowledgement](#) (.doc)

4.17 Asset Management

Asset Management, maintained by VDSS DIS, concerns protection of the components that comprise VDSS systems by managing them in a planned, organized and secure fashion. Asset Management includes Asset Control, Software License Management, Configuration Management, and Change Control.

4.17.1 Asset Control

Asset Control must be commensurate with *sensitivity* and risk, and policies and procedures must be applied accordingly. IT personnel are encouraged to maintain their own records, especially those components that are associated with the BIAs and RA processes. VDSS should ensure Asset Management is a component of the current Asset Management program. Access to asset inventory records should be restricted to a need-to-know basis. IT employees may be of assistance when an asset inventory is conducted since some components are difficult to identify if included within a larger system.

The VITA/NG partnership maintains the inventory of hardware for all of VDSS locations. DIS is then billed for VITA/NG hardware deployed at VDSS locations throughout the state. It is not mandated by VITA/NG or DIS that VDSS sites maintain an inventory listing. Still, all of VDSS locations and offices have certain responsibilities to promote the ability for inventory to be properly managed.

There are several processes DIS uses to identify possible inventory errors. DIS routinely “spot checks” for accuracy as well as investigates discrepancies. These processes help detect idle equipment, old equipment, assets assigned to an incorrect location or function, refresh activities as well as other inventory-related activities. Assets will be researched for business necessity and proper use. DIS will utilize and maintain a POC list for all VDSS locations and contact them as necessary to address any inventory concerns or questions.

Related References:

Equipment - Adding Existing Equipment to State Inventory

[IT Asset Management Policy and Procedures \(.doc\)](#)

[Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard \(.pdf\)](#)

[Surplus Computer Equipment Removal Request \(.doc\)](#)

4.17.2 Software License Management

Maintenance of proper security software requires that all VDSS division/directorate/office/district/regions and LDSS take necessary steps to ensure proper software and documentation is maintained for all COV systems. Only the VDSS-approved software may be installed on VDSS IT systems. Non-VDSS provided software may be installed on VDSS computers if approved by the NG Service Level Director (SLD) and the VDSS CISO.

- **IMPORTANT!** LDSSs are responsible to maintain an accurate accounting of all locally purchased software and ensure compliance with all aspects of the vendor licensing agreement(s).
- Before installing any non-standard software on a state computer, complete the software request form and e-mail it to security@dss.virginia.gov. Once approved, call the VITA Customer Care Center (VCCC) and request that a technician install the software.
- *NOTE: State software cannot be provided for locally-owned servers, desktop or laptop computers.*

Related References:

[IT Asset Management Policy and Procedures \(.doc\)](#)

[Non-VDSS Provided Software Request \(.doc\)](#)

4.17.3 Configuration Management and Control

Configuration Management and Change Control practices must be in place so that changes to the IT environment do not compromise VDSS security controls. Configuration Management is required per the *VDSS Software Development Lifecycle Manual (SDLM)* via the Project Management Plan.

Note: All change requests must be submitted in writing through the Service Request (SR) process within the ITIM process for the VDSS.

Related References:

[Business Process Re-Engineering](#)

[Database Change Request \(.doc\)](#)

[Office of Enterprise Delivery Systems \(OEDS\)](#)

Project Management Plan (.doc) – Section 10.4

[Software Development Lifecycle Methodology \(SDLM\)](#)

[Software Development Lifecycle Manual \(.pdf\)](#)

[Software Quality Assurance \(SQA\)](#)

5. Compliance

All VDSS division/directorate/office/district/regions and LDSS are responsible for ensuring compliance with IT security policies and standards. VDSS measures compliance with IT security policies and standards through processes that include, but are not limited to:

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

5.1 Monitoring

In support of the Commonwealth's efforts to strengthen the public trust by more effectively monitoring how resources are used, NG invested in a new offering of the latest IT security known as "Blue Coat" service. This enterprise-class technology provides web protection that can be managed at the state level. With the application, VDSS can monitor and create reports, with proper authorization, on internet usage by state and local employees. Monitoring of VDSS IT systems and data may include, but is not limited to: network traffic; application and data access; keystrokes and user commands; and e-mail and Internet usage; and message and data content.

SPIDeR:

All searches performed in SPIDeR are logged. The information logged includes, but is not limited to, the worker's LDAP-ID, the date and time of the search, and the data (client's name, Social Security Number (SSN), case number, etc.) on which the search was performed. This allows the VDSS ISRM Office to see what searches a worker has performed. It also allows the VDSS ISRM Office to see which workers have searched for information about a specific client or case.

We suggest each LDSS randomly selects workers each month for a review of their SPIDeR searches. The searches performed by these workers are extracted from the SPIDeR Audit Log and sent to the LDSS' management and SOs. The appropriateness of the searches is then determined by that LDSS' management and SOs.

Inappropriate searches may result in termination of employment, being charged with a federal felony offense, and up to a \$5,000 fine.

5.1.1 General Monitoring Activities

Monitoring is used to improve IT security, to assess appropriate use of VDSS IT resources, and to protect those resources from attack. Use of VDSS IT resources constitutes permission to monitor that use. There should be no expectation of privacy when utilizing VDSS IT resources. VDSS reserves the right to:

- a. Review the data contained in or traversing VDSS IT resources;

- b. Review the activities on VDSS IT resources; and
- c. Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the VDSS CISO.

5.1.2 Requesting and Authorizing Monitoring

Requests for reports cannot be made arbitrarily; they must be for a *justifiable* reason.

The VDSS CISO has the responsibility to authorize monitoring or scanning activities for network traffic; application and data access; keystrokes and user commands; and e-mail and Internet usage; and message and data content for VDSS IT systems and data. The VDSS CISO and the VDSS ISO shall notify each other when appropriate.

Related References:

[Audit Log – Internet/EAL/SPIDeR Request \(.docx\)](#)

Enterprise Audit Log (EAL) Policy, May 2012, Information Security and Risk Management

6. Process for Requesting Exception to the Information Security Policy

If the Commissioner determines that compliance with the provisions of the *COV IT Security Policy* or related standards would result in a significant adverse impact to VDSS, the Commissioner may request approval to deviate from that security policy requirement by submitting an exception request to the COV CISO.

If division/directorate/office/district/regions and LDSS management determines that compliance with the provisions of the VDSS ISPSGs 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 security policy requirement by submitting an exception request to the VDSS CISO.

Each 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 VDSS CISO or the VDSS ISO 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.