Virginia Department of Social Services

Information Security Policy

Revised: May 2008

PREFACE

Subject

VDSS Information Security Policy

Effective Date: June 1, 2008

Compliance Date: July 1, 2008

Publication Revision History

Original	July 15, 1992
Revision 1	April 3, 2001
Revision 2	November 18, 2003
Revision 3	May, 2007
Revision 4	May, 2008 – **Revision changes indicated with Blue Text**

Authority

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

Code of Virginia § 2.2-603(F) (Authority of Agency Directors)

Code of Virginia, §2.2-2827 (Restrictions on state employee access to information infrastructure)

Code of Virginia §2.2-3803 (Administration of systems including personnel information; Internet privacy policy)

Code of Virginia, §2.2-3800
(Government Data Collection and Dissemination Practices Act)

Code of Virginia, Chapter 52

TANIF 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

USDA/FNS 7 CFR .72.1(c), 272.1(d), Disclosure of Information

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

Public Law 100-235, Computer Security Act of 1987

Virginia Social Service Laws 63.2 (2002)

Virginia State Library and Archives, Records Retention and Disposition Schedules (RM-2) (7/94)

ITRM Policy SEC500-02

ITRM Standard SEC501-01

Scope

This policy applies to:

All *Individuals* (VDSS employees, employees of local social service agencies (LSSA), contractors, vendors, volunteers, work experience personnel and other persons and organizations) who have a need to use DSS related information or information processing systems;

All information and information processing systems associated with the Department of Social Services; and

All information and information processing systems associated with other organizations which the Department of Social Services uses, including but not limited to SSA, TAX, IRS, DMV, and VEC.

In accordance with the *Code of Virginia* § 2.2-603, § 2.2-2009, and § 2.2-2010 the VDSS is responsible for complying with Commonwealth ITRM policies and standards and considering Commonwealth ITRM guidelines issued by the CIO. In addition: *"The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in, 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 information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence."*

Regulatory References

1. Privacy Act of 1974.
2. Internal Revenue Codes 6103(d), 6103(b)(4), and 6103(p).
3. Social Security Act paragraphs 464 and 1137.
4. Children's Online Privacy Protection Act.
5. Family Educational Rights and Privacy Act.
6. Executive Order of Critical Infrastructure Protection.
7. Federal Child Pornography Statute: 18 U.S.C. & 2252
8. FDA CFR 21, Part 11.
9. Executive Order 13231
10. USA Patriot Act of 2001.
11. Bank Secrecy Act.
12. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3.,4., 5., and 6.
13. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85.
14. California Database Breach Notification Act.
15. Federal Information Security Management Act (FISMA).
16. Notification of Risk to Personal Data.
17. Office of Management and Budget (OMB) Circular A-130.
18. Tax Information Security Guidelines For Federal, State and Local Agencies Publication 1075

Definitions See Glossary

TABLE OF CONTENTS

1. INFORMATION SECURITY POLICY STATEMENT

1.1 Background

The Virginia Department of Social Services (VDSS) relies heavily on the application of information technology for the effective delivery of benefit and 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.

a. Information is:

   1. A critical asset that shall be protected.

   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.

   6. Everybody's responsibility.

1.3 Purpose

The purpose of the DSS Information Security Policy is to:

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

b. Make each of us aware of our 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's rights and remedies in the event of such a loss.

1.4 Statement of Policy

The Commissioner is responsible for the security of the Department's data including case records and documents containing client or confidential information; and for taking appropriate steps to secure Department IT systems and data through the Department's Information Security Program. This policy and related standards provides the minimum security requirements that apply to all divisions, offices and local social service agencies. Exceptions to this policy must be clearly documented, reviewed and approved by the VDSS Information Security Officer (ISO).

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

a. Ensure confidentiality of department information by protecting department information and information systems against unauthorized access or disclosure;

c. Maintain the integrity of department data;

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

e. Meet federal, state and other regulatory and legislative requirements; and

f. Ensure business continuity in the event of a catastrophic event.

Violations of this policy must be reported to the appropriate division/office/agency director and the VDSS Information Security Officer. Depending on the severity, an employee who violates these policies may receive a Standards of Conduct Offense. 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 use any VDSS related information, information processing systems or equipment for fraudulent, extortive or destructive purposes.

In the case of lost or missing computer equipment or software, notification must also be made immediately to the Information Security Officer.

2. ROLES AND RESPONSIBILITIES

2.1 Policy

Each division, office, region, district and local social service agency must have an effective security administration function in place. For an information security program to be effective, someone in each division, office, region, district and local social service agency 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.

Each division, office, district, region and local social service agency must designate a security officer and at least one backup security officer whose responsibility is to ensure compliance with the VDSS Information Security Policies and Standards.

2.2 Commissioner

The Commissioner is responsible for the security of the Department's Information Technology (IT) systems and data including case records and documents containing client or confidential information. The Commissioner, through the Information Security Unit, is responsible for assuring that Information Security Policies are developed and distributed to all VDSS and local social service agency staff, contractors, vendors and other persons and organizations who have a need to use VDSS related information and information processing systems. The Commissioner is responsible for final interpretation of this policy.

The Commissioner's responsibilities include the following:

a. Designate an Information Security Officer and Backup Information Security Officer for the Department and ensuring the shortest practicable reporting lines to the Commissioner.

b. Maintain an IT security program that is sufficient to protect the Department's IT systems and the program is documented and effectively communicated.

c. Approve a business impact analysis (BIA), a risk assessment (RA), and a Continuity of Operations Plan (COOP) to include an IT disaster recovery plan.

d. Facilitate the communication process between data processing staff and those in other areas of the Department.

e. Establish a program of IT security safeguards.

f. Establish and provide for an IT security awareness and training program

g. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

h. Maintain compliance with IT Security Audit Standards.

i. Accept residual risk as described in section 2.5 of the IT Security Audit Standard (COV ITRM Standard SEC5007-00).

j. Review the IT System Security Plan for each sensitive agency IT system, and disapprove those that do not provide adequate mitigation of risks to which the IT system is subject.

2.3 Division/Office/District/Regional/Local Agency Management

Managers at all levels are responsible for the security of the Department's 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 IT security to the highest level necessary for resolution.

Division, office, district, regional and local social service agency directors are responsible for:

a. Appointing security officers and backup security officers;

b. Implementing, and enforcing procedures within their units which ensure compliance with VDSS Information Security Policies and Standards;

c. Ensuring violations or suspected violations of VDSS Information Security Policy are reported to the DSS Information Security Officer; and

d. Ensuring that all users of VDSS information and information systems are made aware of VDSS Information Security Policies and Standards and receive continuing security training.

2.4 All Personnel

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

a. Reading and complying with the Department of Social Services' Information Security Policies.

b. Reading and signing the: Information Security Policy, Standards and Acceptable Use Awareness Acknowledgement document.

c. Doing everything reasonable within their power to ensure that the Department's Information Security Policy is implemented, maintained, and enforced.

d. Reporting breaches of information security, actual or suspected, to appropriate management and the VDSS ISO.

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

2.5 Information Security Officer (ISO)

The Information Security Officer is responsible for developing and managing the Department's Information Security Program. The ISO duties are as follows:

a. Develop and manage an IT security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.

b. Develop and maintain an IT security awareness and training program for Department and local social service agency staff, including contractors, volunteers and service providers.

d. Coordinate and provide IT security information to the VITA CISO as required;

e. Implement and maintain the appropriate balance of protective, detective and corrective controls for VDSS IT systems commensurate with data sensitivity, risk and system criticality.

f. Mitigate and report all IT security incidents in accordance with §2.2-603 of the *Code of Virginia* and VITA requirements and take appropriate actions to prevent recurrence.

g. Maintains liaison with the Commonwealth's CISO.

h. Verify and validate that all agency IT systems and data are classified for sensitivity.

2.6 VDSS Information Security Unit

The VDSS Information Security Unit is responsible for providing technical information, security assistance, and fostering and overseeing the Department's information security program. Specific responsibilities include but are not limited to:

a. Providing technical assistance to divisions, offices, districts, regions and local social service agencies in developing, implementing and administering their security programs and procedures;

b. Developing, maintaining and disseminating Information Security Polices, Standards and Guidelines, ensuring their uniform interpretation and implementation throughout state VDSS offices and local social service agencies;

c. Participating in VDSS System Development activities to ensure an appropriate level of security, confidentiality and availability is provided to VDSS systems.

d. Performing business impact analysis and risk assessment studies for VDSS' information technology systems;

e. Developing, maintaining and disseminating a disaster recovery plan for the Division of Information Systems and performing an annual disaster recovery test;

f. Training workers on the security features of VDSS' systems; and

g. Reviewing security incident reports and coordinating corrective action to prevent a similar occurrence. Investigate alleged security breaches.

2.7 Security Officers

Division, office, district, regional and local social service agency security officers serve as the point of contact for all security related matters in their divisions, offices and agencies. Security officer 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. Security officers are responsible for:

a. Administering user access privileges to DSS information systems and resources.

b. Verifying the access privileges of active employees.

c. Communicating security-related events to the VDSS ISO.

d. Attending annual security training sponsored by VDSS.

e. Providing security training to their local staff annually.

2.8 System Owner (VDSS Division Directors and their designees)

The System Owner is the Department 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 required IT security awareness and training 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 developing any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.

c. Maintain compliance with VDSS IT security policies and standards in all IT system activities.

d. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

e. Designate a System Administrator for the system.

2.9 Data Owner (VDSS Division Directors and their designees)

The Data Owner is the Department manager responsible for the policy and practice decisions regarding data including case records and documents containing client or confidential information and is responsible for the following:

a. Evaluate and classify sensitivity of the data.

b. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

c. Communicate data protection requirements to the System Owner.

d. Define requirements for access to the data.

2.10 Data Owner (Local Social Service Agency Directors)

Directors of Local Social Service Agency that enter data supplied by VDSS into local systems are responsible for the security of the local Information Technology (IT) systems and data contained therein. The local director is responsible for assuring that Information Security Policies are developed and distributed to all local social service agency 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 IT Security Policy.

The local director's data ownership responsibilities include:

a. Establishing and maintaining an IT security program for local systems that process or store VDSS provided information (i.e. Harmony, EZ-filer) that includes:

- Developing and distributing Information Security Policies and Standards to all individuals who use local systems that process or store VDSS provided information.

- Establishing and providing IT security awareness and training relevant to local systems.

b. Providing for both physical and logical separation of duties by ensuring no one person has sole control of sensitive processes.

2.11 Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

a. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.

b. Establish, monitoring, and operating IT systems in a manner consistent with VDSS IT security policies and standards.

c. Provide Data Owners with reports, when necessary and applicable.

2.12 System Administrators (VDSS Division of Information Systems)

The Systems Administrator is an analyst, engineer or consultant who implements, manages and/or operates a system or systems at the direction of the System Owner and/or Data Custodian. The Systems Administrator assists department management in the day-to-day administration of the department's IT systems and implements security controls and other requirements of the department's IT security program on the IT systems for which the Systems Administrator have been assigned responsibility. Systems administrators are appointed by the Department's Chief Information Officer (CIO).

3. Laws and Penalties

3.1 Laws

Privacy Act of 1974. Provides that unauthorized access to or disclosure of personal information 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). Provides that unauthorized disclosure of any information provided by the 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.

Fair Credit Reporting Act. Under this law, obtaining information under false pretenses or unauthorized disclosure of information is punishable by a fine of up to $5,000 or one year's imprisonment or both. Consumers may also bring civil suit for damages they sustain, and the court may also award a civil penalty of up to $1,000 for knowing and willful violations.

Freedom of Information Act. 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.

3.2 Penalties

Employees who violate the Information Security Policy may be subject to a Standards of Conduct. 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.

4. IT SECURITY PROGRAM

The VDSS ISO is charged with developing and administering the VDSS IT security program in a manner that meets Department 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 the following IT Security Program requirements can be found in the VDSS Information Security Standards. While the majority of these security program components are VDSS' responsibility, those infrastructure related components are the responsibility of VITA/NG.

4.1 Risk Management

This policy and related standards are based on protecting VDSS systems and data based on sensitivity and risk, including system availability needs. Accordingly, Risk Management is a central component of the Department's IT security program and allows the Department to determine how these factors apply to its IT systems.

The first step in Risk Management is a Business Impact Analysis (BIA). BIA is a process of analyzing the Department's business functions, to identify those that are essential or those that contain sensitive data, and assessing the resources that support them. For the purposes of IT security, the BIA identifies those business functions that are essential or involve sensitive data and that are dependent on IT. This analysis is necessary in order to determine the appropriate level of protection for IT systems and the data they process.

After completing the BIA, the Department will document and characterize the types of data it handles, and classify the sensitivity of IT systems and data for use in the Risk Assessment (RA) process. Sensitivity must consider the elements of availability, confidentiality and integrity.

The posting of sensitive data on a public web site is prohibited, unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating logical and physical controls, and any residual risk.

The Department then defines, inventories, and determines ownership of all IT systems classified as sensitive so that IT security roles can be appropriately assigned.

A periodic, formal RA is required for all IT systems classified as sensitive. While a formal RA is not required for IT systems that are not sensitive, an informal risk analysis should be conducted on those IT systems and the data they handle, and to apply appropriate additional IT security controls as required. The RA process assesses the threats to IT systems and data, probabilities of occurrence and the appropriate IT security controls necessary to reduce these risks to an acceptable level.

After appropriate mitigating IT security controls have been applied relative to sensitivity and risk, based on 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. The requirements for IT Security Audits are discussed in more detail in Section 5 of this document, and in the *IT Security Audit Standard* (COV ITRM Standard SEC502-00).

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 Risk Management process is formal acceptance by the Commissioner or designee of any residual risk to Department's operations from sensitive IT systems.

4.2 IT Contingency Planning

IT Contingency Planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and data that support essential business functions if an event occurs that renders the IT systems and data unavailable. IT Contingency Planning includes Continuity of Operations Planning, Disaster Recovery Planning, and IT System Backup and Restoration.

A key element of IT contingency planning is Continuity of Operations Planning, which provides a business continuation strategy for essential VDSS business functions as identified in the BIA. These processes may or may not be dependent on IT resources. The Virginia Department of Emergency Management (VDEM) provides the COV guidance on Continuity of Operations Plans (COOP).

Disaster Recovery Planning supports COOP by defining specific policies, processes, standards, and procedures for restoring IT systems and data that support essential business functions, on a schedule that supports VDSS' mission requirements.

Based on related elements in the IT contingency planning process, IT System Backup and Restoration defines plans and restoration schedules that meet VDSS' mission requirements for the backup and restoration of data.

4.3 IT Systems Security

The purpose of IT systems security is to define the steps necessary to provide adequate and effective protection for VDSS IT systems in the areas of IT Systems Security Plans, IT System Hardening, IT Systems Interoperability Security, Malicious Code Protection, and IT Systems Development Life Cycle Security. The Department's IT systems may require further security controls for adequate protection based on the identification of sensitivity and risk to these systems, including system availability needs, identified through Risk Management policies, processes, and procedures.

Based on the results of the RA, an IT System Security Plan must be developed for each sensitive agency IT system. The IT System Security Plan documents existing and planned IT security controls for the IT System, a schedule for implementing planned IT security controls, and how these controls provide adequate mitigation of risks to which the IT system is subject. The IT System Security Plan must be reviewed and approved by the Agency Head or ISO.

4.4 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.

4.5 Data Protection

Data Protection provides security safeguards for the processing and storing of data. This component of the VDSS 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.

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.

4.6 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.

4.7 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 Security Awareness and Training requirements to provide all IT system users with appropriate understanding regarding VDSS security policies and Acceptable Use requirements for the Department's systems and data.

4.8 Threat Management

Threat Management addresses protection of VDSS systems and data by preparing for and responding to IT security incidents. This component of the Security Program includes Threat Detection, Incident Handling, and IT Security Monitoring and Logging.

When unencrypted personally identifiable information (PII) is subject to a breach in security resulting in unauthorized disclosure, the Department shall provide appropriate notice to affected individuals. This notice should occur without unreasonable delay as soon as verification of a breach is made, consistent with the investigative needs of both COV CIRT and law enforcement entities. The *IT Security Standard*, Section 9.5, provides more information on the notification requirements.

4.9 IT Asset Management

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

5. COMPLIANCE

All Divisions, Offices, Districts, Regions, and Local Social Service Agencies are responsible for ensuring compliance with IT security policies and standards. The Department 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

5.1.1 General Monitoring Activities

Monitoring is used to improve IT security, to assess appropriate use of Department IT resources, and to protect those resources from attack. Use of Department 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 Department IT resources.

b. Review the activities on Department IT resources.

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 CIO.

5.1.2 User Agreement to Monitoring

Any use of Department IT resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed. Users of Department IT resources:

a. Agree to comply with Department policy concerning the use of IT resources;

b. Acknowledge that their activities may be subject to monitoring;

c. Acknowledge that any detected misuse of Department IT resources may be subject to disciplinary action and legal prosecution.

5.1.3 User Monitoring Notification

Where possible, all IT system users will be notified by the display of an authorized Department warning banner that Department IT systems may be monitored and viewed by authorized personnel, regardless of privacy concerns. This notice shall, at a minimum, appear whenever the IT system user first logs on to the IT system and shall be included in IT security awareness training.

5.1.4 What is Monitored?

Monitoring of VDSS IT systems and data may include, but is not limited to: network traffic; application and data access; keystrokes and user commands; e-mail and Internet usage; and message and data content.

5.1.5 Requesting and Authorizing Monitoring

The CISO or ISO when appropriate 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 Department IT systems and data. The CISO and the ISO shall notify each other when appropriate.

5.1.6 Infrastructure Monitoring

Department IT personnel are responsible for maintaining security in their environment through the following processes:

a. Monitoring all systems for security baselines and policy compliance.

b. Notifying the CISO and Department ISO of any detected or suspected incidents.

Note: Installing or using unauthorized monitoring devices is strictly prohibited.

Note: Monitoring the environment infrastructure is a VITA/Northrop Grumman responsibility.

5.2 Internet Privacy

The *Code of Virginia* § 2.2-3803 (B) requires every public body in the COV that has an Internet website to develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public and is consistent with the requirements of the *Code*. VDSS' Internet privacy policy and Internet privacy policy statement can be found on the VDSS public web page.

6. Information Security Audits

6.1 Description

The Code of Virginia § 2.2-2009 gives the CIO the responsibility to *"direct the development of policies, procedures and standards for . . . performing security audits of state electronic information."* These policies are outlined in this section; specific requirements are detailed in the *IT Security Audit Standard* (COV ITRM Standard SEC502-00).

6.2 Performance of IT Security Audits

As required by the *IT Security Audit Standard* (COV ITRM Standard SEC502-00), IT Security Audits (audits) shall be conducted by CISO personnel, VDSS Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of the Department, has the experience and expertise required to perform IT security audits.

Annually, each Department is required to develop and submit to the CISO an audit plan for Department electronic information. Department electronic information is any COV information stored in a format that enables it to be read, processed, manipulated, or transmitted by an IT system.

The audits conducted under the annual VDSS audit plan must measure compliance with this *Information Technology Security Policy* (COV ITRM Policy SEC500-02) and the *Information Technology Security Standard* (COV ITRM Standard SEC501-01). IT Security Auditors also should also use standards that measure compliance with any other applicable federal and COV regulations.

6.3 Documentation and Reporting of IT Security Audits

After conducting the audit, the auditor shall report the audit results to the Commissioner. The Commissioner shall then require the development of a Corrective Action Plan that includes concurrence or non-concurrence with each finding in the audit report as well as the mitigation strategies. At least once each quarter, the Commissioner or designee shall submit to the CISO a report containing a record of all IT Security Audits conducted by or on behalf of the Department during that quarter. The report must include all findings and specify whether the Department concurs or does not concur with each. The report must also include the status of outstanding corrective actions for all IT Security Audits previously conducted by or on behalf of the Department.

7. Protection of IT Resources

The CISO, in conjunction with the Commissioner through the VDSS ISO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of COV IT security laws or policies to preserve evidence that might be utilized in forensic analysis of a security incident.

8. Process for Requesting Exception to IT Security Policy

If the Commissioner determines that compliance with the provisions of the *ITRM Information Technology Security Policy* (COV ITRM Policy SEC500-02) or related standards would result in a significant adverse impact to the Department, the Commissioner may request approval to deviate from that security policy requirement by submitting an exception request to the CISO (see the form attached as the Appendix to this document).

If Division/Office/District/Regional/Local Agency Management determines that compliance with the provisions of VDSS Information Technology Security Polices and Procedures or related standards would result in significant adverse impact to their Division/Office/District/Regional/Local Agency, the director or senior manager may request approval to deviate from that security policy requirement by submitting an exception request to the VDSS ISO (see the form attached as the Appendix to this document).

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 CISO or ISO as appropriate and the requesting party informed of the action taken. Denied exception requests may be appealed to the CIO of the Commonwealth or the CIO of VDSS as appropriate.

9. GLOSSARY

Academic Instruction and Research Systems: Those systems used by institutions of higher education for the purpose of providing instruction to students and/or by students and/or faculty for the purpose of conducting research.

Access: Access: The ability to use, modify or affect an IT system or to gain entry to a physical area or location.

Access Controls: Access controls: A set of security procedures that monitor access and either allow or prohibit users from accessing IT systems and data. The purpose of access controls is to prevent unauthorized access to IT systems.

Accountability: The association of each log-on ID with one and only one user, so that the user can always be tracked while using an IT system, providing the ability to know which user performed what system activities.

Agency Head: The chief executive officer of a department established in the government of the Commonwealth of Virginia.

Alert: Notification that an event has occurred or may occur.

Alternate Site: A location used to conduct essential business functions in the event that access to the primary facility is denied or the primary facility has been so damaged as to be unusable.

Application: A computer program or set of programs that meet a defined set of business needs. See also *Application System.*

Application System: An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application*, *Support System*, and *Information Technology (IT) System.*

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Assurance: Measurement of confidence in a control or activity.

Attack: An attempt to bypass security controls on an IT system in order to compromise the data.

Audit: An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Authentication: The process of verifying an identity of a user to determine the right to access specific types of data or IT system.

Authorization: The process of granting access to data or IT system by designated authority after proper identification and authentication.

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

Backup: The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is damaged or lost.

Business Continuity Plan: A set of processes and procedures to recover an organization's essential business functions in a manner and on a schedule to provide for the ongoing viability of the organization if a disruption to normal operations occurs.

Baseline Security Configuration: The minimum set of security controls that must be implemented on all IT systems of a particular type.

Business Function: A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. See also *Essential Business Function.*

Business Impact Analysis (BIA): The process of determining the potential consequences of a disruption or degradation of business functions.

Change Control: A management process to provide control and traceability for all changes made to an application system or IT system.

Chief Information Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board.

Chief Information Security Officer of the Commonwealth (CISO): The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of IT systems and data.

Commonwealth of Virginia (COV): The government of the Commonwealth of Virginia, and its agencies and departments.

Commonwealth of Virginia Computer Incident Response Team (COV CIRT): A function of the Incident Management division of the COV Security and Risk Management directorate. The COV CIRT operates under the direction of the Incident Management Director, and is primarily comprised of the Incident Management engineers, with additional resources available as needed on a per incident basis from IT Partnership technical, legal and human resources staff.

Computer Emergency Response Team Coordination Center (CERT/CC): a center of Internet security expertise, located at the Software Engineering Institute at Carnegie Mellon University that studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to assist the CERTs of other organizations. See also *Incident Response Team* and *United States Computer Emergency Response Team (US-CERT).*

Confidentiality: The protection of data from unauthorized disclosure to individuals or IT systems..

Configuration Management: A formal process for authorizing and tracking all changes to an IT system during its life cycle.

Continuity of Operations Planning: The process of developing plans and procedures to continue the performance of essential business functions in the event of a business interruption or threat of interruption.

Continuity of Operations Plan (COOP): A set of documented procedures developed to provide for the continuance of essential business functions during an emergency.

Control Objectives for Information and related Technology (COBIT): A framework of best practices (framework) for IT management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control.

Countermeasure: An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an IT system.

Credential: Information, such as a user ID and password passed from and IT system or IT system user to an IT system to establish access rights.

Cryptography: The process of transforming plain text into cipher text, and cipher text into plain text.

Customer-Facing IT System: An IT system designed and intended for by external agency customers and or by the public. COV employees, contractors, and business partners may also use such systems. See also IT System and Internal IT System.

Data: An arrangement of numbers, characters, and/or images that represent concepts symbolically...

Database: A collection of logically related data (and a description of this data), designed to meet the information needs of an organization.

Data Classification: A process of categorizing data according to its sensitivity.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Data Security: Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

Data Sensitivity: See Sensitivity.

Digital Certificate: An electronic document attached to a file that certifies the file is from the organization it claims to be from and has not been modified from the original format.

Digital Signature: A number that uniquely identifies the sender of a message and proves the message is unchanged since transmission.

Disaster Recovery Plan (DRP): A set of documented procedures that identify the steps to restore essential business functions on a schedule that supports agency mission requirements.

Data Storage Media: A device used to store IT data. Examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

Electronic Information: Any information stored in a format that enables it to be read, processed, manipulated, or transmitted by an IT system.

Encryption: The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users..

Essential Business Function: A business function is essential if disruption or degradation of the function prevents the agency from performing its mission as described in the agency mission statement.

Evaluation: Procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

Extranet: A trusted network; used by COV to connect to a third-party provider.

Federal Information Security Management Act (FISMA): Federal legislation whose primary purpose is to provide a comprehensive framework for IT security controls in Federal agencies.

Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Function: A purpose, process, or role.

Group: A named collection of IT system users; created for convenience when stating authorization policy.

Group-based Access: Authorization to use an IT system and/or data based on membership in a group.

Harden: The process of implementing software, hardware, or physical security controls to mitigate risk associated with COV infrastructure and/or sensitive IT systems and data.

High Availability: A requirement that the IT system is continuously available, has a low threshold for down time, or both.

Identification: The process of associating a user with a unique user ID or login ID.

Incident Response Capability (IRC): The follow-up to an incident including reporting, responding and recovery procedures.

Information: Data organized in a manner to enable their interpretation.

Information Security Officer (ISO): The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's IT security program.

Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Assurance: Measures that protect and defend information and IT systems by providing for their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Technology (IT) Contingency Planning: The component of Continuity of Operations Planning that prepares for continuity and/or recovery of an organization's IT systems and data that support its essential business functions in the event of a business interruption or threat of interruption.

Information Technology (IT) Infrastructure Library (ITIL): A framework of best practice processes designed to facilitate the delivery of high quality information technology (IT) services.

Information Technology (IT) Security: The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Architecture: The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems and data.

Information Technology (IT) Security Audit: The examination and assessment of the adequacy of IT system controls and compliance with established IT security policy and procedures.

Information Technology (IT) Security Auditor: CISO personnel, agency Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the agency, has the experience and expertise required to perform IT security audits.

Information Technology (IT) Security Breach: The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system.

IT Security Event: An occurrence that has yet to be assessed but may affect the performance of an IT system.

Information Technology (IT) Security Incident: An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Incident Response Team: An organization within an agency constituted to monitor IT security threats and prepare for and respond to cyber attacks. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *United States Computer Emergency Response Team (US-CERT).*

Information Technology (IT) Security Logging: Chronological recording of system activities sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or

leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

Information Technology (IT) Security Policy: A statement of the IT Security objectives of an organization, and what employees, contractors, vendors, business partners, and third parties of the organization must do to achieve these objectives.

Information Technology (IT) Security Program: A collection of security processes, standards, rules, and procedures that represents the implementation of an organization's security policy

Information Technology (IT) Security Requirements: The types and levels of protection necessary to adequately secure an IT system.

Information Technology (IT) Security Safeguards: See *Information Technology (IT) Security Controls.*

Information Technology (IT) Security Standards: Detailed statements of how employees, contractors, vendors, business partners, and third parties of an organization must comply with its IT Security policy.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control. See also *Application System* and *Support System.*

Information Technology (IT) System Sensitivity: See Sensitivity.

Information Technology (IT) System Users: As used in this document, a term that includes COV employees, contractors, vendors, third-party providers, and any other authorized users of IT systems, applications, telecommunication networks, data, and related resources.

Integrity: The protection of data or IT system from intentional or accidental unauthorized modification.

Internal IT System: An IT system designed and intended for use only by COV employees, contractors, and business partners. See also IT System and Customer-Facing IT System.

Internet: An external worldwide public data network using Internet protocols to which COV can establish connections.

Intranet: A trusted multi-function (data, voice, video, image, facsimile, etc.) private digital network using Internet protocols, which can be developed, operated and maintained for the conduct of COV business.

Intrusion Detection: A method of monitoring traffic on the network to detect break-ins or break-in attempts, either manually or via software expert systems.

Intrusion Detection Systems (IDS): Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Intrusion Prevention Systems (IPS): Software that prevents an attack on a network or computer system. An IPS is a significant step beyond an IDS (intrusion detection system), because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

ISO/IEC 17799: An IT security standard published in 2005 by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). It provides best practice recommendations on IT security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

Key: A sequence of data used in cryptography to encrypt or decrypt information

Key Escrow: The process of storing the encryption key with a third-party trustee to allow the recovery of encrypted text.

Least Privilege: The minimum level of data, functions, and capabilities necessary to perform a user's duties.

Logon ID: An identification code (normally a group of numbers, letters, and special characters) assigned to a particular user that identifies the user to the IT system.

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying IT systems and/or data. Malicious code includes viruses, Trojan horses, trap doors, worms, spy-ware, and counterfeit computer instructions (executables)..

Malicious Software: See Malicious Code.

Management Control: A set of mechanisms designed to manage organizations to achieve desired objectives.

Mission Critical Facilities: The data center's physical surroundings as well as data processing equipment inside and the systems supporting them that need to be secured to achieve the availability goals of the system function.

Monitoring: Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

Non-repudiation: A characteristic of a message that validates that the message was sent by a particular organization or individual, and cannot be refuted.

Off-site Storage: The process of storing vital records in a facility that is physically remote from the primary site. To qualify as off-site, the facility should be at least 500 yards from the primary site and offer environmental and physical access protection.

Operational Controls: IT security measures implemented through processes and procedures.

Operational Risk: The possibility of loss from events related to technology and infrastructure failure, from business interruptions, from staff related problems and from external events such as regulatory changes.

Out-of-Band Communications: A secondary communications channel for emergencies and/or redundancy.

Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Personal Digital Assistant (PDA): A digital device, which can include the functionality of a computer, a cellular telephone, a music player and a camera

Personal Identification Number (PIN): A short sequence of digits used as a password.

Personally Identifiable Information (PII): Any piece of information that can potentially be used to uniquely identify, contact, or locate a single person.

Personnel: All COV employees, contractors, and subcontractors, both permanent and temporary.

Phishing: A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

Privacy: The rights and desires of an individual to limit the disclosure of individual information to others.

Privacy Officer: The privacy officer, if required by statute (such as HIPPA) provides guidance on the requirements of state and federal Privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the IT system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Risk: The potential that an event may cause a material negative impact to an asset.

Risk Analysis: A systematic process to identify and quantify risks to IT systems and data and to determine the probability of the occurrence of those risks

Risk Management: Identification and implementation of IT security controls in order to reduce risks to an acceptable level

Recovery: Activities beyond the initial crisis period of an emergency or disaster that are designed to return IT systems and/or data to normal operating status.

Residual Risk: The portion of risk that remains after security measures have been applied.

Restoration: Activities designed to return damaged facilities and equipment to an operational status.

Risk: The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA): The process of identifying and evaluating risks so as to assess their potential impact

Risk Mitigation: The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk

Role-based Access Control: A type of access control in which IT system users receive access to the IT systems and data based on their positions or roles in an organization.

Roles and Responsibility: Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This document contains the roles and responsibilities associated with implementing IT security.

Recovery Time Objective (RTO): The amount of time targeted for the recovery of a business function or resource after a disaster occurs.

Secure: A state that provides adequate protection of IT systems and data against compromise, commensurate with sensitivity and risk.

Sensitive: See Sensitivity.

Sensitivity: A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that compromise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause.. IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

Sensitivity Classification: The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire

process. It is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

Shared Accounts: A logon ID or account utilized by more than one entity.

Spy-ware: A category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

State: See *Commonwealth of Virginia (COV).*

Support System: An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also *Application System* and *Information Technology (IT) System.*

System. See *Information Technology (IT) System*

System Administrator: An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the operation and maintenance of an agency IT system.

Technical Controls: IT security measures implemented through technical software or hardware.

Third-Party Provider: A company or individual that supplies IT equipment, systems, or services to COV Agencies.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token: A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

Trojan horse: A malicious program that is disguised as or embedded within legitimate software.

Trusted System or Network: An IT system or network that is recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

United States Computer Emergency Response Team (US-CERT): A partnership between the Department of Homeland security and the public and private sectors, intended to coordinate the response to IT security threats from the Internet. As such, it releases information about current IT security issues, vulnerabilities and exploits as Cyber Security Alerts, and works with software vendors to create patches for IT security vulnerabilities. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *Incident Response Team.*

Universal Serial Bus (USB): A standard for connecting devices.

Untrusted: Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

USB Flash Drive: A small, lightweight, removable and rewritable data storage device.

User ID: A unique symbol or character string that is used by an IT system to identify a specific user. See Logon ID.

Virginia Department of Emergency Management (VDEM): A COV department that protects the lives and property of Virginia's citizens from emergencies and disasters by coordinating the state's emergency preparedness, mitigation, response, and recovery efforts

Version Control: A management process that provides traceability of updates to operating systems and supporting software.

Virus: See Malicious Code.

Virginia Information Technologies Agency (VITA): VITA is the consolidated, centralized IT organization for COV.

Vital Record: A document, regardless of media, which, if damaged or destroyed, would disrupt business operations.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Workstation: A terminal, computer, or other discrete resource that allows personnel to access and use IT resources.

APPENDIX A – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM (for state agencies)

Any Agency requesting an exception to any requirement of this policy and the related Standards must submit the form on the following page.

IT Security Policy & Standard Exception Request Form

Date of Request: _____

Requester: _____ Agency Name: _____

IT Security Policy or Standard to which an exception is requested:
_____

In each case, the Agency requesting the exception must

1. Provide the **Business or Technical Justification** for not implementing the Standard**:**

2. Describe the scope and extent of the exception:

3. Identify the safeguards to be implemented to mitigate risks associated with the exception:

4. Define the specific duration of the exception (not to exceed six (6) months):

Approved _____ _____
Agency Head Date

Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____
CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____
Agency Head Date

Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date

APPENDIX B – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM (for VDSS use)

Any Division/Office/District/Regional/Local Social Service Agency requesting an exception to any requirement of this policy and the related Standards must submit the form on the following page.

IT Security Policy & Standard Exception Request Form

Date of Request: _____

Requester: _____ Division/Office/District/Regional/Local Social Service Agency**: _____**

IT Security Policy or Standard to which an exception is requested:

_____

In each case, the Division/Office/District/Regional/Local Social Service Agency requesting the exception must

1. Provide the **Business or Technical Justification** for not implementing the Standard**:**

2. Describe the scope and extent of the exception:

3. Identify the safeguards to be implemented to mitigate risks associated with the exception:

4. Define the specific duration of the exception (not to exceed six (6) months):

Approved _____ _____
Agency Head Date

Information Security Officer of the Commonwealth (ISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____
ISO Date

Division/Office/District/Regional/Local Social Service Agency **Request for Appeal Use Only**

Approved_____ Comments:

_____ _____
Division/Office/District/Regional/Local Social Service Agency Director Date

VDSS Chief Information Officer (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date