



# **FSSA POLICY**

## **SYSTEM AND INFORMATION INTEGRITY POLICY**

EXECUTIVE POLICY #: 2014-012-IT

Effective Date: **October 5, 2014**

### **Revision History**

Version 1.0 – July 01, 2014: Initial policy created for comment period.

Version 1.1 – August 28, 2014: revisions applied.

### **Purpose**

The purpose of this policy is to establish integrity measures and procedures regarding information system configuration, security, and error handling. Implementation of control mechanisms decreases the risk that unauthorized users will gain access to FSSA information systems. The policy statements below contribute to the FSSA information security program by enumerating the best practices with regard to system configuration, security, and error handling controls. This policy serves to supplement Indiana Office of Technology, Indiana Code and any applicable federal compliance statutes.

### **Scope**

This policy applies to information systems in use at FSSA.

### **Definitions**

#### **Application**

An application is composed of one or more pieces of computer programs. Applications may perform functions in an automated fashion using clearly defined rules to facilitate business goals and meet objectives. Applications require special consideration due to the sensitivity of the information they create, manipulate, maintain, or transmit.

#### **CVSS**

The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. It was developed by a coalition of security professionals from around the world representing the commercial, non-commercial, and academic sectors. CVSS is used commonly to prioritize vulnerability remediation activities and calculate a score which communicates the overall severity of vulnerability discovered on one's systems.

### **Information systems**

Information systems are identified by constructing logical boundaries around a set of processes, communications, assets, applications, storage locations and related components. These components collect, store, and process data. FSSA information systems are used to help the agency effectively and efficiently deliver human and social services.

### **IRS Publication 1075**

Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (PDF) contains specific requirements for safeguarding federal tax information.

### **Malicious code**

Malicious code is computer code, software or programs that cause security breaches or damage to information systems. This includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats, contained within compressed files and is found on many forms of media such as USB devices, diskettes, or compact disks.

### **MARS-E**

The Centers for Medicare & Medicaid Services Minimum Acceptable Risk Standards for Exchanges contains specific requirements that address Privacy and Security standards.

### **National Vulnerability Database**

The NVD is the U.S. government repository of standards-based vulnerability management data. This repository includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics

### **Privileged system user**

An individual that is responsible for complying with all security requirements in order to obtain access to an information system. Privileged users (e.g. root or administrator) have a unique role within an organization as they are granted rights within the computer system which are significantly greater than those available to the basic system users.

### **Protected information**

Protected information is a catch-all phrase for certain types of data, material, and facts that are linked to an individual which are protected under state or federal law. Information protected by Health Insurance Portability and Accountability Act of 1996 [Public Law 104-191] (HIPAA) is called Protected Health Information (PHI). Information protected under IC 4-1-6 or IC 4-1-11 is called Personally Identifiable Information (PI/PII). Federal Tax Information (FTI) is any tax return-derived information received from the Internal Revenue Service. Identifiable client data is referred to as client personal information (CPI) in the FSSA Privacy & Security Compliance Policies manual.

### **Security controls**

Security controls are safeguards or countermeasures intended to offset or minimize security risks. The security control guidance is selected from “The Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement”. The MARS-E is based on NIST SP 800-53 with additional controls of IRS Publication 1075 to address the handling of

IRS Federal Tax Information (FTI). The controls for the most part share significant similarity to the NIST 800-53.

### **System Owner**

The system owner is defined as an individual or group of individuals with responsibility for having the information system operated and maintained. System owners coordinate and oversee the successful execution of sound operating practices thereby insuring compliance to established security policies. System owners obligate their service provider or vendor providing service to adhere to legal and regulatory requirements regarding applicable programming, database, and hardware standards. Information system administrators, analysts, developers, engineers, or consultants are obligated to operate, implement, and/or manage an information system on behalf of a system owner in a manner that ensures the confidentiality, integrity and availability of FSSA client data.

### **References**

Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement - <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Catalog-of-MinAcceptable-Risk-Controls-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>

FSSA Privacy & Security Compliance Policies - [http://intranet.fssa.in.gov/SiteCollectionDocuments/LinkedFiles/HIPAA/FSSA\\_Privacy\\_Compliance\\_Policies.pdf](http://intranet.fssa.in.gov/SiteCollectionDocuments/LinkedFiles/HIPAA/FSSA_Privacy_Compliance_Policies.pdf)

IOT Information Security Framework - <http://in.gov/iot/2339.htm>

IOT Technical Requirements - <http://www.in.gov/iot/2394.htm>

IOT Two Factor Authentication Practice - [http://intranet.iot.in.gov/security/Shared/Documents/Practice 8.4.1 - 2 factor authentication.pdf](http://intranet.iot.in.gov/security/Shared/Documents/Practice_8.4.1_-_2_factor_authentication.pdf)

IRS Publication 1075 Safeguards for Protecting Federal Tax Returns <http://www.irs.gov/pub/irs-pdf/p1075.pdf>

NIST Special Publication 800-53 (Rev. 4) Control - Security and Privacy Controls for Federal Information Systems and Organizations - <http://web.nvd.nist.gov/view/800-53/Rev4/>

NIST Special Publication 800-114 - User's Guide to Securing External Devices for Telework and Remote Access - <http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf>

## **Policy Statement(s)**

The existing FSSA Application Security Policy standards already references several applicable SI<sup>1</sup> controls regarding the acceptance of validated [SI-10] input from authorized individuals [SI-9] in a manner which handles invalid data appropriately [SI-11]. Handling and retaining information within and output from the FSSA information system should always occur in accordance with applicable federal laws, directives, policies, regulations, standards, and operational requirements [SI-12].

The following standards further establish effective implementation of integrity measures and procedures regarding information system configuration, security, and error handling.

### **FSSA System and Information Integrity Standards**

1. FSSA shall have a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance which shall be reviewed and updated as necessary every three-hundred-sixty-five (365) days [SI-1].
2. FSSA information systems must be scanned and tested for information system flaws. Software updates, system security patches, service packs, and hot fixes related to flaw remediation must be tested for effectiveness and potential side effects on a non-production information system before installation. Flaw remediation activities must be integrated into the organizational configuration management process and actively managed centrally [SI-2]. Flaws rated as high severity based on the NVD severity rating must be addressed within seven (7) calendar days, medium severity must be addressed within fifteen (15) calendar days, and all others within thirty (30) calendar days.
3. Where possible FSSA should employ automated mechanisms to install software updates automatically [SI-2(1)] to remediate flaws. Similarly, a monthly schedule of automated scanning mechanisms should be executed to determine the presence of flaws in information system components [SI-2(2)].
4. Centrally managed malicious code scanning software [SI-3(1)] must be configured to perform critical system file scans every twenty fours (24) hours [SI-3]. Malicious code protection mechanisms (including signature definitions) should update automatically [SI-3(2)] and prevent non-privileged users from circumventing malicious code protection capabilities [SI-3(3)].
5. FSSA shall insure that intrusion detection tools and devices [SI-4] are organized and interconnected into a system wide intrusion detection system using common protocols [SI-4(1)]. Information system monitoring tools must be automated to facilitate near real-time analysis of events [SI-4(2)] and monitor inbound/outbound communications [SI-4(4)] for unusual conditions. Conditions especially unusual that require near real-time alerting are [SI-4(5)]:
  - a. Presence of malicious code,

---

<sup>1</sup> MARS-E SI System and Information Integrity Control Family

- b. Unauthorized export of information,
- c. Signaling to an external information system, or
- d. Potential intrusions.

4. The FSSA Privacy and Security Office shall pursue and receive information asset security alerts, advisories, and directives from designated external organizations on an ongoing basis. The office shall disseminate internal security alerts, advisories, and directives as necessary to system owners and stakeholders on an ongoing basis as necessary [SI-5].

5. FSSA information systems shall employ automated integrity verification tools to look for evidence of information tampering, errors, and omissions [SI-7] daily [SI-7(1)].

6. FSSA information systems shall be protected from spam at key entry and exit points [SI-8] via a centrally managed [SI-8(1)] solution.

**Exemption(s):**


Exemptions to this policy will be determined by the FSSA Privacy & Security Officer and the principals involved. Exemptions or exceptions to component configuration settings are made after consideration of the security commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of data or information systems.

**Enforcement:**

Noncompliance with this policy and stated implementation standards may result in loss of data access privileges, systems being taken offline, or personnel sanctions in accordance with state and FSSA policy.

**Roles and Responsibilities:**

FSSA is responsible for adhering to the security standards, procedures or guidelines referenced by the above policy.

Authorized by:  on: 8/29/14  
John J. Wernert, M.D., Secretary Date