



# **FSSA POLICY**

## **APPLICATION SECURITY POLICY**

EXECUTIVE POLICY #: 2014-003-IT

Effective Date: **August 31, 2014**

### **Revision History**

Version 1.0 – May 9, 2014: Initial policy created for comment period.

Version 1.1 – June 23, 2014: revisions applied.

### **Purpose**

The purpose of this policy is to ensure the integrity of information which is created, manipulated, maintained, or transmitted by FSSA applications; to protect the confidentiality of FSSA client data; and insure the availability of FSSA data. This policy establishes standards for application software developed, purchased, sourced or currently in use by the FSSA.

Software applications that are designed and created with secure coding tools and techniques have significantly fewer vulnerabilities, bugs or flaws. Security vulnerabilities in application software contribute to data theft and loss. FSSA client personal information must be protected from theft, unauthorized change, destruction, or disclosure, whether intentional or accidental.

This policy serves to supplement Indiana Office of Technology, Indiana Code and any applicable federal compliance statutes. This policy is not intended to supersede any existing policies in place.

### **Scope**

This policy applies to applications 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.

#### **Data Confidentiality Categories**

As per the IOT data characterization reference, there are four confidentiality categories: confidential, sensitive, private and public. The implementation and execution of security

safeguards and controls for applications varies depending on the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to information.

### **Secure code standards**

Secure code standards are specific rules and guidelines that document correct utilization of programming languages. These recommendations for building reliable secure programs when employed by developers minimize the number of vulnerabilities produced in the code at the time of the standard's publication.

### **Programming languages**

Languages are formatted instructions, words, phrases or symbols that are read and translated into machine code so that a computer may execute them. Examples of programming languages are C, C++, Java, or C#.

### **References**

IOT data characterization practice 4.2.2 - [http://intranet.iot.in.gov/security/Shared Documents/Practice 4.2.2 - Data Categorization.pdf](http://intranet.iot.in.gov/security/Shared/Documents/Practice%204.2.2%20-%20Data%20Categorization.pdf)

IOT technical requirements - <http://www.in.gov/iot/2394.htm>

IOT Information Security Framework - [http://intranet.iot.in.gov/security/Shared Documents/Practice 8.2.1 - End User Password Minimums.pdf](http://intranet.iot.in.gov/security/Shared/Documents/Practice%208.2.1%20-%20End%20User%20Password%20Minimums.pdf)

FSSA Privacy 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)

NIST Special Publication 800-18 Revision 1 - <http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>

## Policy Statement(s)

Applications in use must meet these minimum FSSA Application Security Standards. Observance of FSSA application security standards, procedures or guidelines does not imply a completely secure application.

### FSSA Application Security Standards

1. New applications must be developed in accordance with a standards based method of systems development. System security engineering guidelines must be included in all aspects of the system lifecycle including but not limited to the specification, design, development, implementation, and modification of the information system. A standards based method of development includes secure code development standards which address general and specific steps to be taken to ensure that secure, reliable and robust code is produced. Application developers must document and have approved all required software to implement a new application. This includes software located on servers and workstations. All modifications to required software must also be included in all relevant documentation.
2. Applications must validate inputs to insure that expected values are entering the system properly. All data that enters the system shall be subject to input validation to insure it is trustworthy. Similarly the information exiting an application must be formatted or encoded correctly upon output.
3. Applications must only send or display data the user is authorized to view, manipulate or alter in accordance with the application's requirements.
4. Applications must account for and utilize reliable and accepted authentication mechanisms. They should be able to perform an authentication against an enterprise class directory service (LDAP) such as the Microsoft Active Directory service available in the IOT infrastructure. Applications should allow for granular role based account security configuration.
5. Applications must allow for capture of events for audit activity. The ability to generate and maintain application logs (to the extent practical) is necessary for meeting the needs of historical record keeping and compliance with all regulations.
6. All applications must be developed with proper error handling routines or "exception management" in place. Applications must not wrongfully disclose system information.
7. Applications must adequately protect users by keeping session times to the minimum duration necessary and performing proper session management to insure that user sessions are neither hijacked nor impersonated by unauthorized parties.
8. Applications not performing an authentication against an enterprise class directory service must provide features and functions that allow for account expiration and renewal.

9. Provide features and functions that will allow it to comply with all [IOT technical requirements](#).

10. Meet or exceed the password guidelines to achieve compliance with relevant security and regulatory standards, laws, directives or regulations.

11. Application vendors must respond to software vulnerabilities by releasing security patches on a schedule that corresponds to vulnerability risk level. Vendor support should include updates for security vulnerabilities and discovered flaws in the each release of application software in use.

12. Applications should not require the elimination or minimization of security controls to achieve performance, scalability or flexibility targets.

13. Sufficient and acceptable encryption must be employed to guard against loss, theft or interception of client personal information. Applications must make use of secure storage techniques to insure that client personal information is not disclosed inadvertently, left exposed unintentionally or available anonymously. Protection for client personal information residing on storage media that comes to rest or is at rest should be provided either through native functionality or sufficiently strong third party encryption tools.

In addition to the above standards:

- All FSSA application software that is installed must be able to pass an internal application scan assessment.
- All FSSA application software that is installed must be able to pass a server vulnerability security scan.
- All FSSA application software must integrate with the priorities defined in the recovery strategies defined for the timely resumption of FSSA business functions.
- All FSSA application software must be capable of achieving compliance with relevant security and regulatory standards, laws, directives or regulations as it relates to the data within the application. For example: FTI – IRS Pub. 1075, PCI DSS, Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

**Exemption(s):**

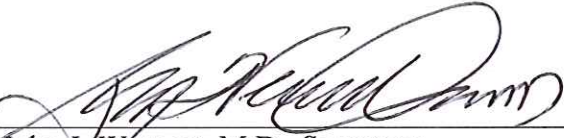
Applications that are exempt from this policy will be determined by the Privacy & Security Officer and/ or delegated manager based on risk and criticality of needed application changes/functionality/architecture.

**Enforcement:**

Any applications that do not adhere to this policy may be taken offline, or have their functionality or access limited to temporarily mitigate an issue, or be denied from entering production service.

**Roles and Responsibilities:**

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

Authorized by:  on: August 1, 2014  
John J. Wernert, M.D., Secretary Date