Michael R. Pence, Governor
State of Indiana

Indiana Family and Social Services Administration

FSSA POLICY

SECURITY PLANNING POLICY

EXECUTIVE POLICY #: 2014-008-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 an enterprise security planning measures and procedures. Security planning helps maintain the confidentiality, integrity and availability of FSSA client data. The policy statements below contribute to the FSSA information security program. An effective information security program improves FSSA's security posture and aligns information security with FSSA's mission, goals, and objectives. This policy serves to supplement Indiana Office of Technology, Indiana Code and any applicable federal compliance statutes.

Scope

This policy applies to FSSA information systems.

Definitions

Availability

Availability is defined as ensuring timely and reliable access to and use of information. A loss of Availability is the disruption of access to or use of information or an information system [44 U.S.C., SEC. 3542].

Confidentiality

Confidentiality is defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information [44 U.S.C., Sec. 3542].

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.

Information system security categorization

System security categorization relies upon the identification of the types of information stored or created within a system and determining the expected impact from a loss in confidentiality, integrity, and availability. An impact level of low, medium or high is determined for each type of information stored or created within a system. The overall impact level for the system is based on these impact levels for confidentiality, integrity, and availability.

Security Objective	Potential Impact		
	Low	**Moderate**	**High**
CONFIDENTIALITY	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe, catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
INTEGRITY	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe, catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
AVAILABILITY	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe, catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 1: FIPS 199 Categorizations

Integrity

Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information [44 U.S.C., Sec. 3542].

IRS Publication 1075

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

MARS-E

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

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.

Security objectives
The three (3) most common security objectives considered for data and information systems are confidentiality, integrity and availability.

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.

System security plan
A system security plan delineates the responsibilities and expected behavior of all individuals who access an information system. It is documentation of the structured process for planning adequate, cost-effective security protection for a major application or information system.

Rules of behavior
The specifications and conditions users agree to follow as part of interacting with or using an information system are known as rules of behavior. Rules over behavior cover topics such as connection limits, remote access, information usage, assignment of system privileges and consequences for inappropriate behaviors.

References

Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems - http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FSSA Privacy & Security Compliance Policies - http://intranet.fssa.in.gov/SiteCollectionDocuments/LinkedFiles/HIPAA/FSSA_Privacy_Compliance_Policies.pdf

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

NIST Special Publication 800-18 - Guide for Developing Security Plans for Federal Information Systems - http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.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 800-60 - Guide for Mapping Types of Information and Information Systems to Security Categories - http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf and http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf.

Policy Statement(s)

The FSSA security planning standards specify that system security plans must be created. A system security plan delineates the responsibilities and expected behavior of all individuals who access a system. System security plans must reflect the current level of protection of information resources within an information system. Robust plans provide the greatest assurance to system owners that an information system is ready to operate. Authorization by a system owner that an information system is ready to operate and process information indicates that the system owner accepts the associated risk of running the information system discussed in the system security plan.

FSSA Planning Standards

1. FSSA shall review, update, and disseminate the security planning policy every three-hundred-sixty-five (365) days [PL-1, CP-2].
2. FSSA's system security plans shall at a minimum include the following [PL-2]:
   a. A title page, document history and updated table of contents which correspond to the respective system of interest.
   b. An introduction that includes the suggested audience, the information system security categorization, the contact information for the system owner and key contacts.
   c. An enumeration of any confidentiality requirements relevant to the data created by, passing through or stored in the system.
   d. A description of the operational environment for the information system including hardware, software, and (if appropriate) networking/ telecommunications equipment. The description must reflect any environmental or technical factors that are of security significance.
   e. A detailed list of the relationships with or connections to other information systems; including applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high level design).
   f. Lists and descriptions of physical and environmental security controls at facilities including those at the back-up site.
3. System security plans shall be reviewed every three-hundred-sixty-five (365) days and updated minimally every three (3) years to address current conditions or whenever [PL-2]:
   a. There are significant changes or problems are identified during plan implementation or security control assessments.
   b. When the data sensitivity level increases.
   c. After a serious security violation due to changes in the threat environment.
4. FSSA security plans must enumerate the rules of behavior for system users. The rules must adequately account for user roles and responsibilities [PL-4].
5. Wherever FTI is incorporated into an information system that is a data warehouse then security plans must consider IRS Pub. 1075, Exhibit 11 specifications.

6. Wherever data, categorized as Protected Health Information (PHI), is incorporated into a system, the security plan must address document retention policies and procedures relating to HIPAA 164.306.
7. FSSA shall plan and coordinate security-related activities in order to reduce the impact on organizational operations, assets, and users. Security-related activities include, for example, security assessments, audits, table top simulations, system hardware and software maintenance, and contingency plan testing [PL-6].
8. FSSA system security plans may reference other key security-related documents for the information system such as risk assessments, plan of action and milestones, any applicable privacy impact assessments, system contingency plan, checklists, or system interconnection agreements as appropriate.

Exemption(s):

Exemptions for applications or information systems will be determined by the FSSA Privacy & Security Officer and the principals involved. Exemptions will be considered only 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:

Violations of standards, procedures or guidelines established pursuant to this policy are considered serious matters. 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