Michael R. Pence, Governor
State of Indiana

Indiana Family and Social Services Administration

FSSA POLICY

GENERAL INFORMATION SECURITY POLICY

EXECUTIVE POLICY #: 2014-013-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 general security policy is to safeguard the integrity, confidentiality and availability of FSSA client data. The following information security policy statements address the various security and risk control objectives embraced by FSSA.

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

Active content

Active content adds functionality and enables dynamic interaction thereby enabling certain electronic documents to carry out or trigger actions automatically without an individual directly or knowingly invoking the actions. Documents which may contain active content would be: PDF(s); Web pages conveying or linking to mobile code; desktop application files containing macros; and HTML encoded email.

Collaborative computing devices

Devices such as networked white boards, cameras, and microphones that are connected to State of Indiana networks and systems utilized for the purposes of conducting government business collaboratively.

MARS-E

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

Media
Media is defined as readable and/or writable end user devices or computer materials capable of being moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); tapes, cartridges, optical platters and discs such as CD, DVD and higher capacity formatted media; floppy disks and software disks.

Mobile code
Mobile code is defined here as software, programs, or scripts obtained from external systems, transferred across a network, downloaded and executed on a local system without explicit installation or execution by the end user. Each form of mobile code has a different security model and configuration management process. Examples of mobile code are: PDF script, Postscript, Shockwave movies, Flash, Java, JavaScript and VBScript. Mobile code is highly utilized on websites on the Internet. Web browsers provide capabilities for mobile code execution environments natively or via browser plug-ins.

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.

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.

Risk assessment
A risk assessment is a careful study, calculation, and classification performed on a recurring basis to measure and understand the likelihood and impact of all identified threats, dangers and consequences of events using qualitative and quantitative methods.

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

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

Catalog of Minimum Acceptable Risk Controls - 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

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

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

NIST Special Publication 800-30 (Rev 1) - Guide for Conducting Risk Assessments- http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.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/

Policy Statement(s)

The following information security policy statements address the various security and risk control objectives embraced by the FSSA. These statements are intended to minimize damage to FSSA information systems by preventing security incidents and reducing the potential loss of FSSA client data.

FSSA Security Standards

1) Staff, consultants, service providers or vendors supporting FSSA information systems must take significant precautions when working with media. Managing risks from improper media access, media storage, media transport, and inadequate media protection is an essential part of the FSSA information security program.

Media utilized by, on, or in FSSA information systems is subject to formal, documented media protection policies pertinent to each information system [MP-1]. Media shall be subject to access restrictions [MP-2], marked [MP-3], physically secured [MP-4], transported [MP-5] and sanitized [MP-6] in a manner considerate of confidentiality, integrity, and availability of the information. When media is no longer needed or required it shall be sanitized [MP-6] using methods of strength and integrity [MP-6(1)] commensurate with the classification or sensitivity of the information [MP-6(5)].

2) FSSA information system owners shall obligate their service provider or vendor providing service to guarantee that physical and environmental protection policies and procedures for FSSA systems are in place. Formal, documented physical and environmental protection procedures that address purpose, scope, roles, responsibilities, management commitment, and coordination must be in place for FSSA information systems [PE-1]. This includes all aspects of authorizations [PE-2], tracking [PE-8] and any physical or environmental controls [PE-10/11/12/13/14/15].

3) FSSA information systems are subject to risks originating from denial of service, data communication and transfer failures. Service providers or vendors providing system and communications support to the FSSA shall provide policy based protections [SC-1] which are reviewed and updated as necessary at least every three-hundred-sixty-five (365) days in response to these risks. Staff, consultants, service providers or vendors supporting FSSA information systems must refrain (unless approved) from utilizing:

a) Remotely activated collaborative computing devices [SC-15]
b) Unapproved mobile code within information systems [SC-18]
c) Voice Over Internet Protocol technologies [SC-19]

4) FSSA information systems wherever feasible and possible should be partitioned into components. Defense in depth[1] is a practical strategy to employ with all FSSA information

[1] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

systems to minimize impacts to the integrity, confidentiality and availability of FSSA client data in the event a security control fails or vulnerability is exploited [SC-32].

5) FSSA information system owners shall insure that individuals with roles as system analysts, developers, programmers integrate information security into the system development life cycle [SA-3]. FSSA application security policy[2] specifies usage of a standards based methodology of systems development that employs security engineering principles [SA-8] and sound developer security testing processes and procedures [SA-11].

6) FSSA information systems shall be subject to formal, documented risk assessment procedures in order to identify, assess, and manage cyber security risk across the enterprise [RA-1]. FSSA information system owners shall facilitate measurement of risk including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the FSSA information systems and data [RA-3].

7) Risk assessment results must be reviewed within every three-hundred-sixty-five (365) days. Risk assessments themselves must be updated within every three (3) years or whenever there are significant changes to the information system or environment of operation. Updated measures of risk are reflected in FSSA system security plans. System security plans reference information system risk assessment results.

8) All information security issues identified by risk assessment or otherwise must be accounted for in a critical infrastructure and key resources protection plan [PM-8]. Updated and completed plans help the FSSA frame and consider the degree of uncertainty that is tolerated by the agency. The degree of risk tolerance contributes to the development of a comprehensive strategy to manage risk [PM-9] to FSSA operations, information systems and information assets. FSSA shall implement this strategy consistently across the agency. The FSSA Privacy and Security Officer or designate shall facilitate ongoing understanding and acceptance of risk to FSSA information systems [PM-10] as formal security assessments are performed.

9) Managing (i.e., documenting, tracking, and reporting) the security state of FSSA information systems helps refine the set of safeguards needed to protect FSSA information systems that support defined FSSA mission and business processes. The FSSA privacy and Security Officer or designate shall ensure that FSSA information system owners understand the level of adverse impact that could result if a compromise of information occurs [PM-11].

Exemption(s):

Exemptions for applications or information systems from this policy 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.

[2] http://intranet.fssa.in.gov/SiteCollectionDocuments/Policies/SecurityPolicy.pdf

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