SECURITY ASSESSMENT POLICY

EXECUTIVE POLICY #: 2014-006-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 a security and assessment authorization measures and procedures. Implementation of security best practices with regard to enterprise security assessment, authorization, and monitoring 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 all FSSA information systems.

Definitions

Corrective Action Plan (CAP)
A corrective action plan (CAP) is a step by step plan of action that is developed to achieve targeted outcomes for resolution of identified errors. CAP(s) help to identify effective actions that can be implemented to correct error causes and improve processes or methods so that outcomes are more effective and efficient.

External information systems
External information systems are information systems which the FSSA or IOT has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. An external information system may be an Internet kiosk, personally owned phone or tablet device, or public computer in a hotel, library or airport.

Federal Tax Information (FTI)
Federal Tax Information (FTI) is any tax return-derived information received from the Internal Revenue Service.

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.

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

Plan of Action and Milestones (POA&M)
A POA&M is permanent record that identifies tasks to be accomplished in order to resolve security weaknesses. Once a weakness is identified, a plan is created to assess, prioritize, and monitor the progress of corrective actions pertaining to the discovered information security weakness.

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 assessment report
A security assessment is a measurement of the security posture of a system or organization. A typical security assessment relies on examination, review and testing to gauge the security posture of a system or organization.

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

IOT Information Security Framework - http://intranet.iot.in.gov/security/Shared Documents/Practice 8.2.1 - End User Password Minimums.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/

Policy Statement(s)

FSSA Security Assessment Standards describe the security and assessment authorization standards that constitute this policy.

FSSA Security Assessment Standards

1. FSSA shall create and maintain a security and assessment authorization policy which is reviewed and updated as necessary within three-hundred-sixty-five (365) days. Plans satisfactorily scoping the assessment environment, assessment team, and assessment roles and responsibilities shall be developed and distributed. FSSA shall evaluate systems to ensure that security requirements are being met for each system [CA-1].

2. For systems in scope of CMS MARS-E requirements a subset of controls may be tested each year so that eventually all controls are assessed once during the 3-year period. If such a system received, stores, processes or transfers FTI, all controls must be assessed at least annually[1].

3. Any newly implemented system should have its security controls assessed prior to being given the authorization to begin processing FSSA data. Afterwards FSSA shall assess a subset of the security controls applied to an information asset on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system [CA-2].

5. FSSA shall ensure that external information systems connections are documented and monitored to insure that information flows to the correct destination(s) or from the intended source(s). The connection documentation shall address the need for links with FSSA systems and the security controls required and implemented to protect the confidentiality, integrity, and availability of the FSSA systems and data flows [CA-3].

6. FSSA shall produce a security assessment report documenting the result of the assessment and provide the result of the security control assessment, in writing, to at a minimum the system owner and designated personnel [CA-2]. Once a weakness is identified, a plan must be created to assess, prioritize, and monitor the progress of corrective actions pertaining to the discovered information security weakness. The CMS MARS-E Plan of Action and Milestones (POA&M) format may be utilized for assessing, prioritizing, and monitoring the progress of these corrective actions.

7. For FSSA systems in scope of CMS MARS-E requirements, a Plan of Action and Milestones (POA&M) [CA-5] must be utilized to document the planned remedial actions to correct weaknesses or deficiencies noted during an assessment (internal/external audit/review or test) of system security controls and to reduce or eliminate known vulnerabilities in the system. The POA&M(s) must be tracked, maintained and submitted to CMS in a timely manner.

[1] 9.3.4.2 Security Assessments (CA-2) http://www.irs.gov/pub/irs-pdf/p1075.pdf

8. For FSSA systems that receive, store, process or transfer FTI, the agency must submit updated Corrective Action Plans (CAPs) twice each year to address corrective actions identified either during an on-site safeguards review or as identified by the IRS until all findings are closed.

9. FSSA shall monitor implemented security controls to demonstrate that they are sufficient and functioning as intended. Discovered vulnerabilities must be tracked over time and remediated appropriately. Security controls and control enhancements are subject to independent assessment [CA-7].

Exemption(s):

Exemptions from 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