Michael R. Pence, Governor
State of Indiana

Indiana Family and Social Services Administration

FSSA POLICY

INFORMATION SYSTEMS MAINTENANCE POLICY

EXECUTIVE POLICY #: 2014-011-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 measures and procedures regarding information system asset maintenance and repair activities. Keeping FSSA information systems in good working order minimizes risks from hardware and software failure. 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

Controlled maintenance

Tasks performed on an information system or components (software or hardware) which are scheduled and performed in accordance with manufacturer, vendor or agency specifications.

Corrective maintenance

When a system abruptly fails or generates an error condition a corrective maintenance task is performed to repair or replace failed components (software or hardware) so the system can be restored to an operational condition as soon as possible. Corrective maintenance may be performed by in-house personnel or outside vendors under a service agreement.

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.

Internal Revenue Service Publication 1075
Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (PDF) contains specific requirements for safeguarding Federal Tax Information (FTI). Federal Tax Information (FTI) is any tax return-derived information received from the Internal Revenue Service

Local system maintenance
Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection from an off-site location.

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

Non-local system maintenance
Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Preventive maintenance
Controlled tasks performed on an information system or components (software or hardware) that are designed to prevent failure are preventive maintenance. Upgrades, patches, or cleaning of parts, components, or materials during off-peak hours are examples of preventive maintenance which minimize information system and component failures.

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 -
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

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

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

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

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 FSSA maintenance policy standards define the measures that help the agency implement best practices with regard to enterprise system maintenance and repair activities.

FSSA Maintenance Standards

1. FSSA shall have documented procedures and/or guides and handbooks to facilitate the implementation of this system maintenance policy which shall be reviewed and updated as necessary every three-hundred-sixty-five (365) days [MA-1].

2. FSSA information systems must have records of maintenance and repairs that demonstrate alignment with manufacturer or vendor specifications. Maintenance activities performed on FSSA information systems must be coordinated and controlled. FSSA information assets or system components must not be moved off-site from facilities for maintenance or repairs without approval from the system owner. Prior to removal from facilities for off-site maintenance or repairs equipment must be sanitized to remove all information from associated media. Following any maintenance activity security controls must be checked to verify functionality [MA-2].

3. For FSSA systems in scope of the CMS MARS-E or IRS Publication 1075 requirements records of maintenance must contain at a minimum[MA-2(1)]:

> a) The date and time of the maintenance activity.
>
> b) The name of the individual performing the maintenance or if necessary the name of employee escort for the maintenance technician.
>
> c) A description of the maintenance performed.
>
> d) A detailed list of equipment removed or replaced including identification, control, or serial numbers.

4. Information system maintenance tools carried into a facility by personnel for usage on in scope systems must be checked for obvious improper modifications [MA-3(1)]. Media containing diagnostics software must be scanned for malicious code (e.g. virus, malware, Trojan) before the media is utilized as part of maintenance and repair activities for systems in scope of the CMS MARS-E or IRS Publication 1075 requirements [MA-3(2)].

5. Any non-local system maintenance must be approved by the system owner and employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions [MA-4]. If password-based authentication is used during remote maintenance of FSSA systems in scope of the CMS MARS-E or IRS Publication 1075 requirements passwords must be changed following each remote maintenance service.

6. Maintenance personnel must either have the required access authorizations or be supervised by designated organizational personnel with the required access authorizations. Individuals supervising maintenance personnel must be technically competent in order to supervise information system maintenance [MA-5].

7. FSSA information system owners shall obligate their service provider or vendor providing service to guarantee that spare parts for systems or components deemed highly critical are available within twenty-four (24) hours of failure. Service providers or vendors providing service shall maintain a list of security-critical information system components and/or key information system technology components to be kept as on-hand spare parts or readily available parts within twenty-four (24) hours of a failure [MA-6]. A failure that stops an entire information system from working jeopardizes FSSA's objective to minimize risks from hardware and software failure.

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:

Assessment and validation procedures shall ensure enterprise system maintenance and repair activities are utilizing security best practices. 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