



FSSA POLICY

SYSTEM CONTINGENCY PLANNING POLICY

EXECUTIVE POLICY #: 2014-009-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 enterprise contingency planning measures and procedures. Contingency planning helps FSSA execute a coherent, organized, planned and strategic response to information system emergencies and other disruptive information system events. 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

Business impact analysis

A business impact analysis (BIA) identifies and prioritizes information systems and components critical to supporting the organization's mission/business processes. Information system service level objectives, restoration priorities, and metrics are often collected for the creation of a business impact analysis.

External information systems

External information systems are information systems which the organization or agency 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.

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 contingency planning

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption.

IRS Publication 1075

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

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.

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

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)

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

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 Contingency Planning policy statements enumerate the standards which contribute to the establishment of a contingency planning capability. This capability will enable FSSA to better respond to information asset failures, system disruptions and disasters. FSSA must develop these plans in regards to business continuity and disaster recovery actions for FSSA information systems.

FSSA Contingency Planning Standards

1. FSSA shall require that information system contingency planning procedures applicable to individual information systems be created. These documented procedures and/or guides and handbooks must address purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities. Completed plans shall be reviewed within every three-hundred-sixty-five (365) days [CP-1].
2. FSSA information system contingency plans shall at a minimum include [CP-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 document's purpose, suggested audience, and list of key terms.
 - c. An enumeration of essential business functions and associated contingency requirements for the system of interest along with an outline of the recovery objectives, restoration priorities, and metrics.
 - d. A complete enumeration of contingency roles, responsibilities, and assigned individuals with contact information.
 - e. A complete list of the essential business functions that must continue in despite of disruption, compromise, or failure of system components.
 - f. Step-by-step restoration procedures or guidance for restoring the impaired system which do not downgrade the security measures originally planned and implemented with the system.
3. FSSA Information system contingency plans should be provided to appropriate individuals as necessary or as identified by name or role. It is imperative that the FSSA respond coherently to an unplanned event, information system outage or information system emergency condition.
4. FSSA information system owners shall review the system contingency plans within every three-hundred-sixty-five (365) days or sooner to address any changes in systems hardware, software or infrastructure.

5. FSSA shall coordinate contingency plan development with appropriate individuals responsible for related plans (e.g., plans for business continuity, disaster recovery, continuity of operations, business recovery, and incident response) [CP-2(1)].
6. Information system owners shall insure that capacity planning occurs on an ongoing basis. FSSA information systems must have sufficient and adequate information processing equipment, telecommunications gear, and environmental controls at an alternative site to insure that FSSA business functions continue to be performed in spite of information asset failures, system disruptions and disasters [CP-2(2)].
7. FSSA shall insure that all appropriate individuals are trained in their contingency roles and responsibilities within every three-hundred-sixty-five (365) days. Training shall be delivered according to a defined frequency and refreshed accordingly [CP-3].
8. FSSA information system contingency plans must be tested at least every three-hundred-sixty-five (365) days to determine the plan's effectiveness and the organization's readiness to execute the plan. The contingency plan test results must be reviewed; any and all issues noted must be corrected to insure the validity of the plan [CP-4].
9. FSSA's alternative processing site, which is separate from the primary site [CP-7(1)], shall have necessary equipment and supplies as required [CP-7]. For FSSA systems in scope of the CMS MARS-E or IRS Publication 1075 requirements any agreements for alternative processing sites must contain language clearly enumerating the priority of service provided [CP-7(3)]. FSSA information systems at the alternative processing site must have equivalent information security controls as the primary site [CP-7(5)] as well as agreements in-place for satisfactory telecommunication services to be brought up within one (1) week [CP-8] [CP-8(1)] [CP-8(2)].
10. FSSA information systems must have recoverable, accurate and recent backups available should it be necessary to restore data, systems or services in the event of a system disruption. For systems in scope of CMS MARS-E requirements [CP-9]:
 - a. A full backup must be performed weekly to separate media.
 - b. Differential or incremental backups to separate media must be performed every day that a full backup is not performed.
 - c. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are to be stored off-site. Off-site and on-site backups must be logged with name, date, time and action and subsequently tested [CP-9(1)].

11. FSSA information system contingency plans must return information systems to a known state after disruption, compromise or failure [CP-10]. Plans must account for circumstances that inhibit recovery and reconstitution to a known acceptable state [CP-10(3)].

Exemption(s):


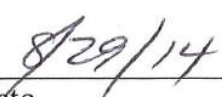
Exemptions will be determined by the FSSA Privacy & Security Officer and the principals involved. The FSSA Privacy & Security Officer and any principals involved shall determine if the contingency plans for systems or individual components within the information system are acceptable [CP-4(1)]. Exemptions 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:

FSSA information systems contingency plans must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. The FSSA Privacy & Security Officer or designate(s) shall review plans for readiness along with system owners to insure that the plans are sound. 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: 
John J. Wernert, M.D., Secretary Date