



# **FSSA POLICY**

## **INFORMATION SECURITY AUDIT AND ACCOUNTABILITY POLICY**

EXECUTIVE POLICY #: 2014-005-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 formal event logging and transaction monitoring capability. Implementing security best practices with regard to logging, monitoring and the retention of audit data helps FSSA insure the confidentiality, integrity, and availability of FSSA client data. 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**

#### **Accountability**

Accountability is the requirement that actions of an entity may be traced uniquely to that entity. Accountability directly supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Unique identification and authentication supports the traceability of duties, actions, and processes of users, operations staff, and management.

#### **Audit**

An audit is a review, examination or objective appraisal of a project, activity, control, or combination thereof that uses a systematic, disciplined approach to gather evidence. Audits are used to assess compliance to a standard or contractual obligation. Auditing helps the agency determine if expectations regarding the confidentiality, integrity and availability of FSSA data are being met.

### **Audit records**

Per NIST SP 800-92 audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, and account changes (e.g. , account creation and deletion, account privilege assignment), and use of privileges.

### **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

### **MARS-E**

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

### **Operating system logs**

Per NIST SP 800-92 operating systems (OS) for servers, workstations, and networking devices (e.g. routers, switches) usually log a variety of information related to security. The most common types of security-related OS logged data are system events and audit records.

### **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 events**

Per NIST SP 800-92 system events are operational actions performed by OS components, such as shutting down the system or starting a service.

## **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.

## **Timestamps (time stamps)**

Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Timestamps are generated by the information system should include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. If time sources other than the system time are used for audit records the timeline of events can get skewed. This makes analysis unreliable. When merging audit logs from several systems, the date and time on those systems must be accurate. Network Time Protocol (NTP) keeps information system clocks accurate and coordinated.

## **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](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 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/>

NIST Special Publication 800-92 Guide to Computer Security Log Management - <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

## **Policy Statement(s)**

The FSSA audit and accountability policy statements define the procedures and actions that help the agency implement event and transaction logging and the retention of audit evidence. These policy standards help the FSSA insure the confidentiality, integrity and availability of FSSA client data.

### **FSSA Audit and Accountability Standards**

1. FSSA shall document the purpose, scope, roles, responsibilities, and management commitment to effectively implement the security controls and control enhancements in the audit and accountability family of controls. These audit and accountability policy statements shall be reviewed and updated as necessary within every three-hundred-sixty-five (365) days [AU-1].
2. FSSA information systems must be capable of generating audit records for the following information system events [AU-2]:
  - a) User account management activities,
  - b) System shutdown / reboot /error(s),
  - c) Application shutdown / restart /error(s),
  - d) File creation/ deletion / modification,
  - e) Failed and successful log-on(s),
  - f) Security policy modifications,
  - g) And use of administrator privileges.
3. Perimeter devices, including firewalls and routers that handle FSSA client data must be capable of generating audit records for the following information events [AU-2]:
  - a) User account management activities,
  - b) System shutdown / reboot /error(s),
  - c) Application error(s),
  - d) Modification of packet filters or proxy services,
  - e) Security policy modifications, and use of administrator privileges,
  - f) Log packet screening denials originating from trusted and un-trusted networks.
4. For systems or devices in scope of the IRS Publication 1075 requirements for FTI, audit records for the following events (in addition to those specified in other controls) must be generated for:
  - a) All successful and unsuccessful authorization attempts,
  - b) All changes to logical access control authorities (e.g., rights, permissions);
  - c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
  - d) The audit trail shall capture the enabling or disabling of audit report generation services;
  - e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database). [AU-12]

4. Each FSSA information system security plan document must define which of the auditable events shown in accountability standard 2 and 3 are capable of being audited. Each system security plan document enumerate the frequency of (or situation requiring) auditing for each identified auditable event [AU-2(3)]. These auditable events must be reviewed for accuracy and completeness within every three hundred sixty-five (365) days.

4. For FSSA information systems in scope of MARS-E requirements execution of privileged functions must be included in the list of events to be audited by the information system. Activities such as including administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors, and access authorizations following control enhancement shall be maintained [AU-2(4)].

5. Audit records must contain sufficient information to, at a minimum, establish
- a) The type of event occurred,
  - b) The date and time the event occurred,
  - c) The location or device where the event occurred,
  - d) The source of the event,
  - e) The outcome (success or failure) of the event,
  - f) The identity of any user/subject associated with the event. [AU-3]

FSSA information systems must be capable of generating audit records for the list of events defined in policy standards two (2) and three (3) with the content defined above in policy standard five (5) [AU-12].

6. FSSA information systems must have sufficient allocated audit record storage capacity to reduce the likelihood of such capacity being exceeded. It is important that relevant documents, records and events not be lost due to insufficient allocation of storage capacity [AU-4].

6. In the event of an audit processing failure personnel listed explicitly or by reference in the system security plan must be notified. The system security plan must define if the system should be shutdown, stop generating audit records or overwrite the oldest audit records [AU-5]. If such a system receives, stores, processes or transfers FTI then shutting down the system, stopping the generation of audit reports or overwriting the oldest records is not an appropriate action.

7. FSSA information systems records must be reviewed and analyzed for indications of inappropriate or unusual activity which subsequently must be reported at a minimum to system owners and the FSSA Privacy and Security Officer [AU-6]. Audit review, analysis and reporting processes must be integrated together to support organizational processes for investigation and response to suspicious activities [AU-6(1)]. Implementation standards dictate review of system audit records shall occur on demand but no less than once within a twenty- four (24) hour period for:

- a) Indications of initialization sequence errors and log-on errors;
- b) Indications of inappropriate or unusual system processes;
- c) Anomalies regarding system performance or resource utilization;

- d) Unusual network traffic, excessive bandwidth utilization rates, and alerts notifications from border defense devices;
- e) Any other suspicious activity or suspected violations.

In addition, implementation standards recommend:

- a) Use of automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior.
- b) Inspection of administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.
- c) Manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

8. Audit reduction and reporting tools must not alter original audit records or log data [AU-7]; original audit records must be protected from unauthorized access, modification, and deletion [AU-1].

9. FSSA information systems must synchronize internal information system clocks daily and at system boot [AU-8] to insure that time stamps are accurate. Time stamps in the individual audit records from FSSA information systems must be reliably related to the time stamps in other audit records to achieve an accurate ordering of recorded events [AU-12(1)].

10. Audit records for FSSA information systems which do not contain FTI shall be retained for at least ninety (90) days and audit records shall be archived for at least one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and information retention requirements.

For FSSA information systems which contain PII, audit inspection reports and corrective action records shall be retained for a minimum of three (3) years from the date the inspection was completed.

For FSSA information systems in scope of the IRS Publication 1075 requirements standardized records of request for disclosure of FTI must be maintained for at least five (5) years and audit information must be archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored [AU-11].

**Exemption(s):**


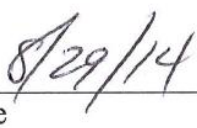
Exemptions to this policy will be determined by the FSSA Privacy & Security Officer and the principals involved. Exemptions or exceptions to component configuration settings shall be made after consideration of the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of data or information systems.

**Enforcement:**

Assessment and validation procedures shall ensure enterprise system event logging and transaction monitoring activities are being performed according to 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:   
John J. Wernert, M.D., Secretary Date