



# Family & Social Services Administration Information Security Policies

Version 3.0

Effective: January 3, 2025

## Table of Contents

Table of Contents.....	2
Introduction—Information Security Policies .....	3
<i>Purpose</i> .....	3
<i>Application</i> .....	3
<i>Background</i> .....	3
<i>Premise</i> .....	3
<i>Availability/Distribution</i> .....	3
Section 1: Policy on Policies and Procedures.....	5
Section 2: General Information Security Policy.....	7
Section 3: Access Control Policy.....	9
Section 4: Application Security Policy.....	12
Section 5: Information Security Audit and Accountability Policy .....	16
Section 6: Configuration Management Policy .....	20
Section 7: System Contingency Planning Policy .....	22
Section 8: Identification and Authentication Policy.....	25
Section 9: System Information and Integrity Policy.....	27
Section 10: Information Systems Maintenance Policy.....	29
Section 11: Security Assessment Policy .....	31
Section 12: Security Planning Policy .....	34
Section 13: Information Technology Risk Management Policy.....	37
Section 14: Definitions.....	40
Section 15: Policy Administration .....	52
Section 16: Signature Page.....	53

# Introduction—Information Security Policies

### ***Purpose***

The purpose of the following Information Security Policies is to establish the rules and procedures to be followed by the Family & Social Services Administration (FSSA) and its personnel to ensure the security, confidentiality and integrity of such information, and protect against unauthorized access to or use of client information that could either:

- Result in substantial harm or inconvenience to any client; or
- Present a safety and soundness risk to the institution.

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 policies, Indiana Code and any applicable federal compliance statutes.

### ***Application***

These Information Security Policies apply to all FSSA divisions, bureaus, sections, facilities (including State Operated Facilities), and program areas and all FSSA personnel (workforce members). These Policies apply to all forms of client personal information, including electronic and paper, and as may be included in verbal communications.

### ***Background***

By the very nature of its business, FSSA creates, obtains, uses, and maintains a significant amount of client personal information, including health information, on individuals who are the beneficiaries of FSSA's services. This includes client personal information on former beneficiaries and those applying for services, as well as personal information on persons associated with current and former beneficiaries and those applying for services (e.g., parent and guardian information).

FSSA is obligated under both federal and Indiana state laws and regulations to protect the confidentiality and integrity of a client's personal information in its safekeeping. This is a substantive responsibility that the agency takes very seriously. It is also a complex responsibility given the scale and scope of the agency and the population we serve.

### ***Premise***

FSSA has many business units that operate under both agency-wide policies and procedures and policies and procedures unique to each unit. Agency-wide policies establish a set of rules applicable to all components of the agency and all agency personnel. These rules are necessary to ensure consistency among the various FSSA business units and staff with respect to the ongoing protection of client personal information, and the agency's ongoing compliance with the various federal and state laws and regulations applicable to the agency as whole.

### ***Availability/Distribution***

These FSSA Information Security Policies are available to all FSSA personnel and other stakeholders on The Hub website. Updated versions of these Policies and Procedures will be posted to The Hub within five (5) business days of final approval of the updates.

### ***References***

MARS-E - Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
FSSA Privacy & Security Compliance Policies
Indiana Office of Technology (IOT) Tier 1 Control Standards

### ***Exception(s):***

Exceptions from these policies will be determined by the FSSA Privacy & Security Officer and the principals involved. Exceptions will be considered only after consideration of the security commensurate with the risk resulting from the unauthorized use, disclosure, disruption, modification, or destruction of data or information systems.

### ***Enforcement:***

Violations of standards, procedures or guidelines established pursuant to these policies are considered serious matters. Noncompliance with these policies and 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 personnel and system owners are responsible for complying with the security policies, standards, procedures or guidelines contained herein as it applies to their systems and associated business operations.

# Section 1: Policy on Policies and Procedures

### ***Purpose***

FSSA and its business owners creates and maintains policies to establish responsibility, integrity, and accountability in support of the mission of the Department and in compliance with state, local, and federal laws. The Policy on Policies is intended to ensure a transparent process for the creation, approval, review, and revision of all policies, to facilitate broader stakeholder awareness of and engagement with such policies while increasing compliance, and to promote institutional consistency in the presentation and spirit of policies.

### ***Scope***

This Policy pertains to all policies of the department, but differentiates among:

- Policies that govern the department as a whole or broad constituencies thereof, e.g. all staff or all workforce members, or a large group of staff external to the Policy sponsor's division ("Agency-wide policies");
- Policies that only govern specific divisions or departments of the agency ("Unit-level policies")

### ***Policy Statement(s)***

The purpose of this policy is to ensure that FSSA has ready access to well-developed and understandable policies at both the agency-wide, department and business unit levels. Policies that are easy to find, read and understand will:

1. Support the FSSA's mission.
2. Achieve accountability by identifying the units/individuals responsible for policies.
3. Provide workforce members with clear, concise guidelines.
4. Document how FSSA conducts business.

Additionally, any developed policies or policies included herein are subject to both FSSA as a whole and on the individual business or unit level.

### **Policy Development**

1. The Policy Initiator (typically process or business owner) may identify a department-level policy requirement or change and develop it into a policy proposal. If the policy is endorsed, a draft policy is created following the format outlined below.
2. The Policy Owner (typically Division or Office director or a designee) will review the draft policy and consult with various stakeholders regarding the policy's likely impact on the members of the department community, including legal and, if appropriate, FSSA Privacy & Security Officer review.
3. After review and input, the policy is formally approved. Once the policy is approved and signed, the Policy Owner will disseminate the policy to the affected individuals.
4. The Policy Owner will maintain copies of signed department policies and policy revisions and place an electronic copy on the designated policy repository. Version control shall be maintained for all applicable policies.

5. The Policy Owner also notifies responsible and/or affected parties when particular policies are scheduled for review or revision and is available to work with the responsible parties during any phase of the policy development process, including, if applicable, implementation of a training schedule. As identified in the particular policy, the responsible party will monitor compliance and facilitate remedies for noncompliance as directed by the policy.
  - a. Standard policy format ensures clarity and consistency. Although not all policies will contain all of the format elements, department policies will be written and maintained following the format described below:
    - i. Header information: (mandatory element)
      1. Policy name
      2. Purpose
      3. Scope - Identification of resources governed and affected by the policy.
      4. References – any regulatory or internal documentation used in the development of the policy.
    - ii. Policy Statements - Purpose of the policy and the statement of philosophy, position, rule, regulation or direction.
    - iii. Exceptions
    - iv. Enforcement
    - v. Responsible Roles and Responsibilities
    - vi. Definitions
    - vii. Policy Administration – to include revision history (date, individual(s) responsible for revisions, brief explanation of revisions made) and review frequency.
    - viii. Signature Page – to include any applicable stakeholders.

## Section 2: General Information Security Policy

### ***Purpose***

The purpose of this general security policy is to safeguard the integrity, confidentiality and availability of FSSA client personal information (CPI). The following information security policy statements address the various security and risk control objectives employed by FSSA.

### ***Scope***

This policy applies to all FSSA information systems.

### ***Policy Statement(s)***

The following information security policy statements address the security and risk control objectives embraced by the FSSA.

### **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.
2. Media utilized by, on, or in FSSA information systems is subject to formal, documented media protection policies pertinent to each information system. Media shall be subject to access restrictions, marked, physically secured, transported and sanitized in a manner considerate of confidentiality, integrity, and availability of the information. When media is no longer needed or required it shall be sanitized using methods of strength and integrity commensurate with the classification or sensitivity of the information.
3. 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. This includes all aspects of authorization, tracking and any physical or environmental controls.
4. All 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 FSSA shall provide policy-based protections which are reviewed and updated as necessary at least every three-hundred-sixty-five (365) days in response to these risks.
5. Collaborative computing devices: Networked collaborative computing devices (e.g., networked whiteboards, cameras, and microphones) may be employed when explicitly authorized by the division director (or designee) provided such devices cannot be remotely activated and provides explicit indication of use to users physically present.

6. Mobile Code: It is the responsibility of the system owner to define and approve mobile code employed in their information systems (e.g., Java, Adobe, JARs, Flash, etc.) and not employ any mobile code backlisted by IOT.
7. FSSA information systems hosted by IOT shall be deployed in a three-tier architecture physically separating the presentation, application, and database components. For information systems hosted by IOT, IOT is responsible for any additional physical component partitioning (e.g., separation of server racks). For information systems hosted by a third-party vendor, the vendor is responsible for any additional physical component partitioning as demonstrated by their FedRAMP certification.
8. All information systems shall be subject to formal, documented risk assessment procedures in order to identify, assess, and manage cyber security risk across the enterprise. 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. [See Information Technology Risk Management Policy, Section 13]
9. 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. [See Information Technology Risk Management Policy, Section 13]
10. All information security issues identified by risk assessment or otherwise must be accounted for in a critical infrastructure and key resources protection plan. Updated and completed plans help 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 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 as formal security assessments are performed. [See Information Technology Risk Management Policy, Section 13]
11. 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.
12. FSSA business unit staff who support information systems that maintain CPI are required to report these systems the Indiana Office of Technology (IOT). FSSA business unit staff are required to provide annual status updates to IOT regarding the operations of these information systems. The FSSA Privacy & Security Office can be consulted for assistance in this reporting process.



### Section 3: Access Control Policy

#### ***Purpose***

The purpose of this policy is to establish access control measures and procedures over FSSA information systems.

#### ***Scope***

This policy applies to FSSA information systems to which access is controlled.

#### ***Policy Statement(s)***

The FSSA access control security standards define the physical and logical access control measures that appropriately limit access to FSSA information, processing systems and facilities to authorized individuals except where designated for public access. The intent of the policy is to provide process and system owners with the appropriate guidelines in order to ensure that appropriate standards are in place.

#### **FSSA Access Control Standards**

1. System owners will prepare documented access control procedures over their systems to facilitate the implementation of the agency access control policy and any additional access controls as deemed necessary and appropriate by the system owner. Such access control procedures are to be annually reviewed by the system owner for continued applicability and reviewed/updated whenever there is a substantive change to the application, supporting infrastructure, access controls, or threat/risk profile.
2. All FSSA information systems will employ role-based access controls. User roles will be defined in accordance with business requirements and assigned job responsibilities, and employ least privilege (i.e., permit access to only the least amount of functionality the role requires to do their associated job); this includes system administrator, database administrator, security coordinator, and similar privileged roles. The information system access control procedures will define the roles, the authorization process for granting access to the information system, and the process for tracking and monitoring role assignments.
3. The information system owner is responsible to review all user accounts every one-hundred-eighty (180) days and modify, disable, or remove any that are invalid, inactive, no longer required or no longer meet the attributes required for the business function. Annually, the information system owner must review and certify all active user accounts are valid and have the appropriate level of access privileges; disabled accounts are to be deleted. Both the semi-annual review and annual certification are to be documented by the information system owner and submitted to the FSSA Privacy & Security Officer. In addition, and to the extent such accounts are under the control of the system owner:

- a. Administrator groups, root accounts, and other system-related accounts are to be inspected at least every fourteen (14) days (and on demand) to ensure unauthorized accounts have not been created.
  - b. Privileged user roles associated with the system (e.g., system administrators, database administrators, security coordinators) should be inspected every thirty (30) days
4. Where technically configurable, system owners are to employ automated mechanisms to support the management of information system accounts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers or security coordinators when users are terminated or transferred; using the information system to monitor account usage via audit logs; and, using automated audit log analysis to report atypical system account usage.
5. User accounts must be unique and identify a specific individual or device; to the extent possible the information system should use the unique identifier assigned to the individual by IOT (i.e., user ID comprised of the user's state email address). In addition:
  - a. User ID's are not to be ever reused after the User ID has been removed from the system.
  - b. User ID's are to be disabled after sixty (60) days of inactivity and then deleted during the annual account recertification process. Audit logs of activity associated with User ID's shall be maintained in accordance with Section 4 of this policy.
  - c. Non-user accounts (e.g., device or service accounts) are typically managed by IOT; in situations where the system owner is responsible for such accounts, inactive non-user accounts are to be disabled after 180 days of inactivity.
6. Temporary and emergency accounts shall be immediately disabled or removed from a system once they are no longer needed (within 24 hours). When temporary accounts are needed for internal or external audit, software development, software installation, training, guest access, or other defined need, the following conditions shall apply:
  - a. Authorized in advance by system owner (via email notification to FSSA Account Control);
  - b. Have a specific expiration date;
  - c. Be monitored while in use;
  - d. Be removed when the work is completed;
  - e. Exist no longer than 365 days.

Training accounts shall be rendered inactive (e.g., by resetting the password) at the end of the training event. If multiple classes are held during a given day, the account may remain active until the end of the day, rather than resetting the accounts between classes held on the same day.

7. Separation of duties: System owners, as part of account management, are responsible to ensure an appropriate separation of duties is in place to limit the opportunity for unauthorized modification or

misuse of information without collusion. For example, auditing of system use should not be performed by personnel who administer access control, system testing is performed by separate groups, and developers are not permitted access to production environments). Separation of duties is to be documented in the system owner's access control procedures.

8. The flow of information between sources and destinations within and between information systems shall be documented and authorized by the system owner, and address the associated security requirements and controls. For example, within the information system data may be protected by encrypted communication channels; reliance on IOT to provide proxy servers and firewalls for external web access, and the use of SFTP and encrypted data for inter-system data exchanges. The confidentiality and integrity of data must be maintained as information moves through multiple systems and boundaries.
9. User accounts will be automatically locked after three (3) consecutive invalid login attempts during a fifteen (15) minute time period; the lockout will persist for at least 30 minutes. Concurrent sessions for each system account must be limited to the number of sessions expressly required for the performance of job duties. Any requirement for more than one (1) concurrent application/process session shall be documented in the respective system's security plan.
10. Remote access to FSSA systems for the purpose of administration or execution of privileged commands shall be for compelling operational needs. Such remote access is only permitted using a VPN (or a similar service) employed by IOT, which requires multi-factor authentication. Permission for such remote access is granted by the system owner and is subject to approval by FSSA Account Control and IOT. The execution of remote access must be audited, documented and approved for all applicable systems.
11. Only FSSA approved systems may be used to process, access, and store FTI, PHI, or PII; private, personal, or non-business information systems shall not be authorized for FTI, PHI, or PII. External information systems may not be utilized to create, manipulate, maintain, or transmit protected information. FSSA approved portable storage devices (approved encrypted USB drives and external hard drives) should not be utilized on external information systems unless they are subject to the restrictions and conditions specified in the FSSA Privacy Compliance Policies & Procedures.
12. Publicly accessible information must not contain non-public information. Only FSSA designated individuals may post information onto an organization information system that is publicly accessible. Any non-public information must be removed from publicly accessible organizational information systems if discovered.

# Section 4: Application Security Policy

### ***Purpose***

This policy establishes minimum security standards for application software developed, purchased, sourced or currently in use by FSSA.

The objective is to assure that applications, whether custom built or off-the-shelf (including externally hosted), incorporate security engineering principles throughout the lifecycle that minimize the risk of the introduction of vulnerabilities and flaws that jeopardize effective operation or expose client data to unauthorized use, disclosure, or modification.

### ***Scope***

This policy applies to all application software developed, purchased, sourced or currently in use at FSSA.

### ***Policy Statement(s)***

It is the responsibility of the system owner to ensure that their applications meet these minimum FSSA Application Security Standards. Observance of FSSA application security standards, procedures or guidelines does not imply a completely secure application.

### ***FSSA Application Security Standards***

1. Custom-built applications must be developed and maintained in accordance with a standards-based systems development lifecycle (SDLC) methodology approved by the system owner. The SDLC must include security engineering guidelines that incorporate a security risk management process to identify security requirements, continuous assessment of risk and risk mitigation, secure coding practices, integrated security testing (both automated and manual), and a documented, overarching security architecture for the application. In addition, the SDLC must address the roles and responsibilities of security personnel throughout the development lifecycle (beginning to end), including maintenance and operations.
2. The application design criteria must incorporate privacy-by-design principles that minimize the risk of the intentional or accidental unauthorized disclosure of client information. These would include, for example, only displaying the minimum amount of client information necessary on a screen (e.g., display only the last four digits of the client's Social Security Number), archiving historical data on a separate database (or other archival storage) to minimize the volume of data that could be subject to a breach, collecting and retaining only the minimum amount of client information necessary for the purpose of the application and associated business processes (i.e., do not collect or retain extraneous data, subject to state/agency/division retention requirements), and employing the masking/redaction/anonymization of data.
3. The system owner is responsible to ensure each application, whether custom-built or off-the-shelf is fully documented, including a System Security Plan (SSP) that defines the security controls to be employed over the application. The security controls employed (and documented in the SSP) must conform to the current version of the applicable MARS-E security and privacy control requirements as

a baseline including, but not limited to, Access Controls, Audit Controls, Configuration Management Controls, Contingency Planning Controls, Identification and Authentication Controls, Risk Assessment Controls, System Acquisition Controls, System and Communication Controls, System and Information Integrity Controls, Data Quality Controls, Data Minimization Controls, and, to the extent applicable based on the hosted environment, Maintenance Controls, Media Protection Controls, and Physical and Environmental Protection Controls.

The SSP should identify those controls inherited from IOT (for IOT-hosted applications) or from the vendor for vendor-hosted applications.

Depending on the content and purpose of the application, the application security controls may be subject to other control requirements, such as IRS Publication 1075 for Federal Tax Information, SSA Technical System Security Requirements for Social Security Administration-obtained information, and Office of Child Support Enforcement for OCSE-obtained information. It is the responsibility of the system owner to ensure all applicable state and federal security control requirements are addressed in the system design and operation.

4. The system owner is responsible to ensure that a security assessment plan is developed and implemented for the application in accordance with the SDLC, the results of which demonstrate with supporting evidence the effective implementation of the applicable security controls as defined in the SSP (reference Section 11)
5. If the application is to be hosted by a vendor (e.g., cloud-based) and contains client information, the vendor's hosting environment must be FedRAMP certified at the moderate level. The system owner is also responsible to assess and document the associated risk prior to employing a vendor-hosted application.
6. The system owner is responsible to ensure that for custom-built applications both a static and dynamic code scan is performed on the code base on a monthly basis and identified vulnerabilities are addressed (resolved, mitigated, compensated) in accordance with the FSSA Security Assessment Policy.
7. For applications that are hosted by IOT, IOT will provide a monthly infrastructure vulnerability scan and/or access to a vulnerability analysis tool (e.g., InsightVM). The system owner is responsible to ensure identified vulnerabilities are addressed (resolved, mitigated, compensation) in accordance with the FSSA Security Assessment Policy.
8. In addition to the security control requirements identified above, the following present additional controls or control enhancement that the system owner must address in their SSP:
  - a. Applications must only send or display the minimum amount of data the user is authorized to view, manipulate or alter in accordance with the business unit's requirements.
  - b. Applications must account for and use reliable and accepted authentication mechanisms in accordance with IOT and FSSA policy. For applications hosted by IOT, authentication for FSSA

workforce members will be performed against the State's Active Directory service managed by IOT. Applications must provide granular role-based account security configuration (role-based access control—reference the Access Control Policy). Vendor-hosted applications, to the extent possible, should use IOT's Active Directory service for authentication (coordination with IOT on the methods and means will be required).

- c. Applications must allow for capture of events for audit activity in accordance with the FSSA Information Security Audit and Accountability Policy. The ability to generate and maintain application logs is necessary for investigative purposes, meeting the needs of historical record keeping, and compliance with all applicable regulations. Audit logs will be retained in accordance with State/Agency retention requirements or as otherwise required under applicable federal regulations.
- d. Applications must employ a session lock after fifteen (15) minutes of inactivity and the lock is to be retained until the user re-authenticates to the application. Typically, session locks are controlled at the operating system level and, therefore, must be part of the infrastructure design for the application. This is not a screensaver lock.
- e. All applications will comply with all IOT technical requirements, with the exception of vendor-hosted applications. However, vendor-hosted applications will need to comply with the applicable IOT requirements such as authentication via IOT Active Directory, communications channel security, etc.
- f. All applications must meet or exceed the password guidelines in accordance with IOT and FSSA policy.
- g. Application vendors must be contractually obligated to provide security patches on a timely schedule and in response to newly identified vulnerabilities (e.g., as identified by vulnerability scans, published in the National Vulnerability Database, identified by MS-ISAC, or identified by other vendors whose products are employed as part of the application. In addition, application vendors must be contractually obligated to maintain the currency of middleware, mobile code, and other products employed as part of the application (e.g., Java, libraries, web services, Active X, JavaScript, etc.) within two major releases at all times—the objective is to avoid end-of-life risk and the introduction of security vulnerabilities associated with prior versions.
- h. For off-the-shelf applications, the system owner is required to maintain the currency of the application at all times to avoid end-of-life risk and the introduction of security vulnerabilities associated with prior versions. All desktop software shall adhere to IOT's standards for allowable versions.
- i. The elimination or minimization of security controls to achieve performance, scalability or flexibility targets is prohibited.

- j. Client personal information in transit and at rest will be encrypted employing FIPS 140-2 or 140-3 compliant encryption protocols and ciphers and with appropriate signed certificates from a valid certificate authority. Typically, IOT will provide cryptographic key management for IOT-hosted applications.

# Section 5: Information Security Audit and Accountability Policy

### ***Purpose***

The purpose of this policy is to establish the requirements for audit logging and monitoring of FSSA applications and infrastructure. The ability to generate and maintain application and system event logs is necessary for investigative purposes, meeting the needs of historical record keeping, and compliance with all applicable regulations.

### ***Scope***

This policy applies to all FSSA information systems.

### ***Policy Statement(s)***

The FSSA audit and accountability policy statements define the procedures and actions that help the agency implement system event and application audit logging and the retention of audit evidence.

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

1. The system owner is responsible to document in the application System Security Plan (SSP) the security controls and control enhancements in the audit and accountability family of controls to be implemented and maintained for the application and its supporting infrastructure. The audit controls established in the SSP are to be reviewed annually by the system owner for continued applicability and reviewed/updated whenever there is a substantive change to the application, supporting infrastructure, audit controls, or threat/risk profile.
2. The system owner is responsible for assessing the following audit events and determining which events are to be logged, including frequency, with respect to the application and supporting infrastructure based on the application risk assessment, security audit function coordination with other organizational entities (e.g., IOT SIEM correlation), and current threat information and ongoing assessment of risk and documenting the determination in the SSP:
  - a. Server alerts and error messages,
  - b. Log onto system,
  - c. Log off system,
  - d. Change of password,
  - e. All system administrator commands, while logged on as system administrator,
  - f. Switching accounts or running privileged actions from another account, (e.g., Linux/UNIX SU or Windows RUNAS),
  - g. Creation or modification of super-user groups,
  - h. Subset of security administrator commands, while logged on in the security administrator role,
  - i. Subset of system administrator commands, while logged on in the user role,
  - j. Clearing of the audit log file,
  - k. Startup and shutdown of audit functions,
  - l. Use of identification and authentication mechanisms (e.g., user ID and password),



- m. Change of file or user permissions or privileges (e.g., use of `suid/guid`, `chown`, `su`),
  - n. Remote access outside of the corporate network communication channels (e.g., modems, dedicated Virtual Private Network) and all dial-in access to the system,
  - o. Changes made to an applications or database by a batch file,
  - p. Application-critical record changes,
  - q. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility),
  - r. User log-on and log-off (successful or unsuccessful),
  - s. System shutdown and reboot,
  - t. System errors,
  - u. Application shutdown,
  - v. Application restart,
  - w. Application errors,
  - x. Security policy modifications,
  - y. Printing sensitive information,
  - z. Subset of Implementation Standard 1, enable logging for perimeter devices, including firewalls and routers:
    - User log-on and log-off (successful or unsuccessful)
    - Log packet-screening denials originating from untrusted networks
    - All system administration activities
    - Packet-screening denials originating from trusted networks
    - Account creation, modification, or deletion of packet filters
    - System shutdown and reboot
    - System errors; and
    - Modification of proxy services.
- aa. Verify that proper logging is enabled to audit administrator activities.
3. For IOT-hosted applications, the system owner will need to coordinate with IOT regarding the capture, retention, analysis, and content of infrastructure-related system event logs (e.g., Windows Event Logs) pertinent to the security posture of the application, including perimeter security devices such as firewalls and routers. Generally stated, IOT is responsible for the production, capture, content, analysis, and retention of system event logs (excluding application logs in most cases), and for responding to security events identified by such logs. However, depending on the nature of the application (i.e., subject to additional audit controls under federal regulation), IOT may need to adjust the content, capture, analysis, and retention of the system event logs or otherwise comply with applicable federal requirements.
4. The system owner is responsible to identify and document in the SSP the retention period for application and system event logs assuring compliance with applicable federal, state, and agency

records retention requirements. For vendor-hosted applications the system owner will need to contractually ensure the appropriate logs are retained for the required period of time.

- a. At a minimum, audit logs should be retained for 90 days online and then archived for one-year, subject to federal/state/agency retention requirements (e.g., audit records for systems within the scope of IRS Publication 1075 must be retained for 7 years; audit records for systems within the scope of MARS-E must be retained for 10 years).
  - b. All 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.
5. For any systems or devices in scope of the IRS Publication 1075 requirements for FTI, the system owner is responsible for and documenting within the SSP any additional auditing requirements as defined in Publication 1075 or the associated SCSEM's, including audit log retention requirements (e.g. seven years).
6. 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.
7. 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. The system owner is responsible to document in the SSP:
  - a. How audit record storage capacity will be monitored,
  - b. At what point a warning or alert will be generated based on the audit record storage capacity consumption level (e.g., at 80% of capacity),
  - c. How warnings and alerts will be generated in the event storage capacity is nearing capacity to whom (role or name) the warning/alerts will be provided.
8. The system owner is responsible to document in the SSP the action to be taken in the event of an audit processing failure--if the system should be shutdown, stop generating audit records or overwrite the oldest audit records--and whom to notify (role or name) in the event of an audit processing failure.

9. The system owner is responsible to document in the SSP the audit review, analysis, and reporting procedures to be followed and which meet the following minimum requirements:
  - a. Audit records are to be reviewed at least weekly using an automated tool for indications of inappropriate or unusual activity,
  - b. A random sample of audit records is to be manually reviewed on demand but at least every 30 days for indications of inappropriate or unusual activity,
  - c. Adjusts the level of audit review if there is a change in the threat environment,
  - d. Initialization sequences, logons, and errors; system processes and performance; and system resource utilization are to be reviewed to detect anomalies on demand but no less than every 24 hours, with alerts going to defined personnel (roles) defined in the SSP,
  - e. Procedures for investigating suspicious activity or suspected violations (and reporting same in accordance with the FSSA Privacy & Security Compliance Policies),
  - f. Administrator accounts under the control of the system owner should be inspected at least every 14 days to ensure unauthorized accounts have not been created,
  - g. Alerts and anomalies are to be reported to the personnel (roles) identified in the SSP,
  - h. For vendor-hosted applications, the vendor is to be contractually bound to review and analyze system audit records (which may exclude application audit records depending on the situation) at least weekly and report any indications of inappropriate or unusual activity to the system owner (or designee).
10. Audit reduction and reporting tools must not alter original audit records or log data; original audit records must be protected from unauthorized access, modification, and deletion.
11. All information systems must synchronize internal information system clocks daily and at system boot to authoritative time sources as identified by IOT to ensure 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.

# Section 6: Configuration Management Policy

### ***Purpose***

The purpose of this policy is to establish configuration management control measures and procedures.

The policy statements below contribute to the FSSA information security program by enumerating the standards and procedures utilized to document, authorize, manage and control system changes.

### ***Scope***

This policy applies to all FSSA information systems.

### ***Policy Statement(s)***

The FSSA configuration management policy standards help to define the measures needed to document, authorize, manage and control changes to systems. The policy statements below establish a configuration management capability throughout the FSSA for documenting, authorizing, managing, and controlling configuration changes that occur on FSSA information systems.

### **FSSA Configuration Management Standards**

1. The system owner is responsible to have a formal, documented configuration management policy and defined configuration baselines (that may be included in the application SSP) for the application and its components; the policy and baseline configurations are to be updated as necessary and reviewed annually .
2. A complete and accurate inventory of all information systems and components under the purview of the system owner will be fully developed and maintained by the system owner. Inventory records must be updated during installations, removals, and updates. A complete master information system inventory eliminates duplicate and inaccurate records in other collections thereby allowing for consistent and accurate baseline configurations to be developed and maintained. For vendor-hosted applications, the system owner is not responsible for maintaining an inventory of system components over which they have no control.
3. A baseline configuration must be developed, documented, and maintained for FSSA information systems by the system owner. FSSA information system baselines shall establish a common point of reference which are then reviewed and updated based on deviations from the baseline configuration in support of mission needs/objectives. Baseline and security configurations should be based on guidelines available from the National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), the Center for Internet Security (CIS), the Internal Revenue Service SCSEM's, vendors, and other qualified resources.
4. A review of baseline configurations must be conducted annually by the system owner or after major information system changes such as new component installations or software upgrades or operating system upgrades.

5. All information systems shall follow a formal SDLC process to ensure that changes to a system are introduced in a controlled and coordinated manner. The system owner shall record, assess, plan, test, and implement configuration-controlled changes to systems with explicit consideration for security impact.
6. Records of configuration-controlled changes to FSSA information systems shall be maintained and periodically audited. Configuration-controlled changes to FSSA information systems must be coordinated and communicated appropriately. If changes such as upgrades or modifications are applied to FSSA information systems, the security functions must be verified to ensure they continue to operate as intended. Detection of unauthorized, security-relevant configuration changes must be accounted for in the incident response function; detected events must be tracked, monitored, corrected, and available for historical purposes.
7. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications
8. All information systems must provide only essential capabilities. System services, ports, network protocols, and capabilities not explicitly required for system or application functionality must be disabled or restricted. Annually, the system owner is responsible to review the application(s) to identify and eliminate these unnecessary functions, ports, protocols, and/or services.

# Section 7: System Contingency Planning Policy

### ***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.

### ***Scope***

This policy applies to FSSA information systems.

### ***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. System owners must develop these plans in regard to business continuity and disaster recovery actions for FSSA information systems.

### ***FSSA Contingency Planning Standards***

1. All information systems are required to have contingency planning procedures in place, which is the responsibility of the respective system owner. These documented procedures must address purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities. Completed plans shall be reviewed annually by the system owner, or sooner to address any changes in systems hardware, software or infrastructure.
2. Information system contingency plans shall at a minimum include:
  - 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 by the system owner to appropriate individuals as necessary or as identified by name or role. It is imperative that the business unit be able to respond coherently to an unplanned event, information system outage or information system emergency condition.

4. Contingency plan development shall be coordinated with appropriate individuals and business units responsible for related plans (e.g., plans for business continuity, disaster recovery, continuity of operations, business recovery, and incident response), including IOT.
5. Information system owners shall ensure 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 ensure that FSSA business functions continue to be performed in spite of information asset failures, system disruptions and disasters.
6. All appropriate individuals must be annually trained in their contingency roles and responsibilities. Training shall be delivered by the system owner according to a defined frequency and refreshed accordingly.
7. Information system contingency plans must be tested at least annually to determine the plan's effectiveness and the organization's readiness to execute the plan. The contingency plan test results must be documented, reviewed; any and all issues noted must be corrected to ensure the ongoing validity of the plan.
8. For IOT-hosted applications, if the business unit has subscribed to IOT's disaster recovery service in which the application(s) is replicated or recovered at the IOT disaster recovery site (Bloomington, IN), for this alternative processing site IOT will provide the necessary equipment and supplies as required for contingent operations of the application(s) in accordance with the disaster recovery plan.
9. For vendor-hosted applications, it is the responsibility of the system owner to assure appropriate contingency/disaster recovery plans are in place by the vendor relevant to the criticality of the application(s).
10. 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. Alternative processing sites, whether the IOT Disaster Recovery site or a vendor disaster recovery site/solution, must have equivalent security controls as the primary site.
11. All 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:
  - 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.

12. All information system contingency plans must return information systems to a known state after disruption, compromise or failure. Plans must account for circumstances that inhibit recovery and reconstitution to a known acceptable state.



# Section 8: Identification and Authentication Policy

### ***Purpose***

The purpose of this policy is to establish identification and authentication measures and procedures to manage the risk associated with user access and authentication activities. Implementation of strong identification and authorization mechanisms will decrease the risk of unauthorized users gaining access to FSSA information systems.

### ***Scope***

This policy applies to information systems in use at FSSA.

### ***Policy Statement(s)***

The following enumerates the FSSA identification and authentication policy standards and requirements.

### ***FSSA Identification and Authentication Standards***

1. System owners are to identify in their SSP the identification and authentication (IA) controls to be employed over their application(s) that are consistent with these policies and standards and address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements. The IA controls will be reviewed annually by the system owner and reviewed/updated whenever there is a substantive change to the application, supporting infrastructure, IA controls, or threat/risk profile.
2. All users must have unique identifiers (i.e., user ID) and uniquely identify and authenticate into information systems. Authentication of user identities shall be accomplished through the use of strong passwords, tokens, biometrics, multi-factor authentication, or some combination thereof. In addition to identifying and authenticating users at the information system level (i.e., at network logon) identification and authentication mechanisms shall be employed at the application level, when necessary, to provide increased information security for the organization (this may be as simple as the user being uniquely identified in the application and verification by the application that the user has an active state Active Directory account).
3. FSSA information systems must use multifactor authentication for network access to privileged accounts and for remote access to both privileged and non-privileged accounts. Multifactor authentication must employ a device separate from the device used to access the system (e.g., IOT provides Phone Factor for multifactor authentication that requires the user to have a separate device from their workstation/laptop—their phone—to separately verify their identity).
4. Identifiers for devices must be unique and assigned to the intended object (e.g., use of IP addresses to uniquely identify the device), and employ authentication mechanisms for device access (e.g., service accounts). Typically, device identifiers and authentication mechanisms are inherited from IOT for IOT-hosted applications or from the vendor for vendor-hosted applications. FSSA authentication and identification standards prohibit reuse of user or device identifiers for the period to which an identifier is assigned to an active user or device. A device or user identifier shall not be reused until all

previous access authorizations are removed from the information system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired.

5. Information systems that use password-based authentication to authenticate users must:
  - a. Verify, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator (i.e., confirm through procedures the identity of the person receiving their password).
  - b. Automatically force users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one-hundred eighty (180) days.
  - c. Prohibit the use of dictionary names or words.
  - d. Enforce minimum password complexity consisting of at least eight (8) characters with at least one upper-case letter, one lower-case letter, one number, and one special character; system accounts are to be at least 15 characters in length and be comprised of a mixture of upper-case, lower-case, numeric, and special characters.
  - e. Enforce at least a minimum of four (4) changed characters when new passwords are created.
  - f. Encrypt passwords in storage and in transmission.
  - g. Enforce password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum.
  - h. Prohibit password reuse for twenty-four (24) generations prior to reuse.
  - i. Protect authenticator content from unauthorized disclosure and modification.
6. All information systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or misuse by unauthorized individuals.
7. When PKI is employed for authentication, the information system must validate the certificates, enforce authorized access to the corresponding private key, map the authenticated identity to the account of the individual, and maintain a local cache of revocation data (to support path discovery and validation in case of an inability to access revocation information via the network).
8. Authenticators (e.g., passwords) cannot be embedded in applications or access scripts or function keys unless encrypted and even then the practice is highly discouraged unless absolutely necessary (as described in the system owner's SSP).
9. With the exception of access to public information, non-organizational user accounts must follow the same identification and authentication policies as described here.

# Section 9: System Information and Integrity Policy

### ***Purpose***

The purpose of this policy is to establish integrity measures and procedures regarding information system configuration, security, and error handling. Implementation of control mechanisms decreases the risk that unauthorized users will gain access to FSSA information systems.

### ***Scope***

This policy applies to information systems in use at FSSA.

### ***Policy Statement(s)***

The existing FSSA Application Security Policy standards already references several applicable SI controls regarding the acceptance of validated input from authorized individuals in a manner which handles invalid data appropriately. Handling and retaining information within and output from the FSSA information system should always occur in accordance with applicable federal laws, directives, policies, regulations, standards, and operational requirements.

The following standards further establish effective implementation of integrity measures and procedures regarding information system configuration, security, and error handling.

### ***FSSA System and Information Integrity Standards***

1. System owners are to identify in their SSP the system and information integrity (SI) controls to be employed over their application(s) that are consistent with these policies and standards and address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements. The SI controls will be reviewed annually by the system owner for continued applicability and reviewed/updated whenever there is a substantive change to the application, infrastructure, SI controls, or threat/risk profile.
2. Automated mechanisms should be used to install software updates automatically to remediate flaws, where possible. The system owner is responsible to coordinate with IOT for IOT-hosted applications with respect to infrastructure (e.g., operating system and firmware) security and software updates.
  - a. Timelines to remediate known flaws are as follows:
    - i. High risk flaws are to be remediated within 7 days of discovery
    - ii. Moderate risk flaws are to be remediated within 15 days of discovery
    - iii. Low risk (and all other) flaws are to be remediated within 30 days of discovery
3. Centrally managed malicious code scanning software shall be configured to perform critical system file scans every twenty fours (24) hours. Malicious code protection mechanisms (including signature definitions) should update automatically and prevent non-privileged users from circumventing malicious code protection capabilities. For IOT-hosted applications and for state-owned workstations, IOT is responsible for malicious code scanning on the infrastructure devices and workstations; for

non-stated-owned workstations and devices not supported by IOT, it is the responsibility of the system owner to address these malicious code scanning requirements.

4. Intrusion detection tools and devices shall be organized and interconnected into a system wide intrusion detection system using common protocols. Information system monitoring tools must be automated to facilitate near real-time analysis of events and monitor inbound/outbound communications for unusual conditions. Conditions especially unusual that require near real-time alerting are:
  - a. Presence of malicious code,
  - b. Unauthorized export of information,
  - c. Signaling to an external information system, or
  - d. Potential intrusions.

For IOT-hosted and vendor-hosted applications, it is the responsibility of IOT and/or the vendor to provide intrusion detection, perimeter security, zone security, and monitoring (the vendor agreement should address the provision of these controls and alerts to the system owner). The system owner is responsible to implement applicable application monitoring solutions for custom-built software to ensure the proper functioning of internal processes and controls, and to identify anomalous activities that could constitute a security or operational threat.

5. The FSSA Privacy and Security Office shall pursue and receive information asset security alerts, advisories, and directives from designated external organizations on an ongoing basis.
6. The FSSA Privacy and Security Office shall disseminate internal security alerts, advisories, and directives as necessary to system owners and stakeholders on an ongoing basis as necessary.
7. All information systems shall employ automated integrity verification tools to look for evidence of information tampering, errors, and omissions daily. For IOT-hosted and vendor-hosted applications, it is the responsibility of IOT and/or the vendor to provide integrity verification of the infrastructure (e.g., daily integrity scans to detect the installation of new hardware, software, or firmware). The system owner is responsible to implement applicable integrity verification tools for custom-built software.
8. All information systems shall be protected from spam at key entry and exit points via a centrally managed solution. For IOT-hosted and vendor-hosted applications, it is the responsibility of IOT and/or the vendor to provide spam protection mechanisms (the vendor agreement should address these protections and alerts to the system owner). The system owner is responsible to employ spam protection mechanisms for custom-built software.

# Section 10: Information Systems Maintenance Policy

### ***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.

### ***Scope***

This policy applies to all FSSA information systems.

### ***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.

For IOT-hosted and vendor-hosted applications IOT and/or the vendor is responsible to employ applicable maintenance controls over the infrastructure. For information systems for which the FSSA system owner provides all or part of the infrastructure, the following standards apply.

### **FSSA Maintenance Standards**

1. The system owner is responsible to document in the application SSP the maintenance controls to be employed, including adherence to these standards. The maintenance controls are to be reviewed annually by the system owner for continued applicability and reviewed/updated whenever there is a substantive change to the maintenance procedures, application, supporting infrastructure, or threat/risk profile.
2. All 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. Maintenance records must contain, at a minimum:
  - 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.
3. Information system maintenance tools carried into a facility by personnel must be checked for obvious improper modifications. 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.

4. Any non-local system maintenance (i.e., performed remotely by maintenance personnel via a network connection) must be approved by the system owner and employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. If password-based authentication is used during remote maintenance the passwords must be changed following each remote maintenance session. Non-local maintenance sessions must be audited, and the audit records are to be reviewed timely by the system owner (or designee) to identify any anomalies.
5. 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 to supervise information system maintenance.
6. 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. A failure that stops an entire information system from working jeopardizes FSSA's objective to minimize risks from hardware and software failure.

# Section 11: Security Assessment Policy

### ***Purpose***

The purpose of this policy is to establish a security and assessment authorization measures and procedures.

### ***Scope***

This policy applies to all FSSA information systems.

### ***Policy Statement(s)***

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

### **FSSA Security Assessment Standards**

1. The system owner is responsible to document in the application System Security Plan (SSP) the security and assessment authorization controls and procedures to be implemented and maintained for the application and its supporting infrastructure. The controls and procedures established in the SSP are to be reviewed annually by the system owner for continued applicability and reviewed/updated whenever there is a substantive change to the application, infrastructure, assessment procedures, or threat/risk profile.
2. The system owner is responsible to perform a security and privacy assessment over the application and its supporting infrastructure on an annual basis, subject to the following:
  - a. Take into consideration any applicable state or federal requirements with respect to the scope, depth, and frequency of the assessment (e.g., IRS Publication 1075, CMS MARS-E, SSA TSSR).
  - b. Subject to a. above, the system owner may plan to assess a portion of the privacy and security controls in place such that over a three (3) year period all controls are assessed, keeping in mind that the system owner should consider assessing certain controls each year such as access controls, auditing controls, training controls for annual training, contingency planning controls, and incident response controls.
  - c. Subject to a. above, the system owner should consider engaging an independent, third-party assessor on at least a tri-annual basis.
  - d. Prepare a detail assessment plan designed to test each of the controls subject to the assessment by collecting evidence that demonstrates each control is operating as expected; summarize the results in a written assessment report. A copy of the assessment report should be provided to the FSSA Privacy and Security Officer and other stakeholders identified by the system owner; a copy should be retained for six (6) years.

- e. The assessment report is to include a discussion of residual risk accepted by the system owner, which may be separately stated in an Information Security Risk Acceptance document (reference Section 13).
- f. Control weaknesses identified from the assessment are to be identified by the system owner in a Plan of Action & Milestones (POA&M). The POA&M is a corrective action plan that identifies the actions to be taken to remediate the weaknesses identified and the timeframes in which remediate will occur. The risk associated with each weakness is to be identified (following the guidance in NIST Special Publication 800-30 R1). Timelines to remediate weaknesses may be governed by federal requirements (e.g., CMS MARS-E) that are more stringent than the following, which are the maximum timelines permitted:
  - i. High risk control weaknesses are to be remediated within 90 days of discovery
  - ii. Moderate risk control weaknesses are to be remediated within 180 days of discovery
  - iii. Low risk control weaknesses are to be remediated within 365 days of discovery

Note: remediation includes applying additional or compensating controls that would reduce the risk level even though the weakness still exists. These same timelines apply to infrastructure vulnerabilities (from infrastructure scans for IOT-hosted applications) and application code vulnerabilities (from static and dynamic code scans of custom-built applications).

- g. For IOT-hosted applications, IOT will need to participate in the assessment for the relevant infrastructure components (including perimeter security); the system owner is responsible to coordinate with the IOT Center for Compliance Excellence for the assessment.
  - h. For vendor-hosted applications, the vendor is to annually provide the system owner with a copy of their FedRAMP certification and a copy of the supporting SOC II report to demonstrate security controls compliance.
- 3. Any newly implemented system must have its security controls assessed prior to being given the authorization to begin processing FSSA data. This includes performing final infrastructure vulnerability scans (for IOT-hosted applications) and static and dynamic application code scans for custom-build applications. The system owner is responsible to authorize the system before commencing operations, attesting that the system has effectively passed the security controls assessment (control weaknesses are within tolerable limits). The authorization is to be renewed every three years or when substantive changes are made to the system, or when a serious security violation which raises questions about the prior security authorization.
  - 4. External information systems connections must be documented, authorized by the system owner (via the SSP or agreements), and monitored to ensure 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.

5. Implemented security controls shall be monitored on a continuous basis as defined by the system owner in the application's SSP to demonstrate that the controls remain sufficient and functioning as intended. Discovered vulnerabilities must be tracked over time in the POA&M and remediated within the defined timeframes (above). For vulnerabilities discovered through infrastructure vulnerability scans and application dynamic and static code scans, POA&M entries may be consolidated by group, vulnerability type, or a similar means (i.e., individual findings do not need to be listed in the POA&M).

## Section 12: Security Planning Policy

### Purpose

The purpose of this policy is to establish an enterprise security planning measures and procedures. Security planning helps maintain the confidentiality, integrity and availability of FSSA client data.

### Scope

This policy applies to FSSA information systems.

### Information System Security Categorization

Security Objective	Potential Impact		
	Low	Moderate	High
<b>CONFIDENTIALITY</b>	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe, catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>INTEGRITY</b>	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe, catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>AVAILABILITY</b>	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe, catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

**Table 1: FIPS 199 Categorizations**

### Policy Statement(s)

The FSSA security planning standards specify that System Security Plans (SSP) must be created and maintained. The SSP delineates the responsibilities and expected behavior of all individuals who access a system, define the characteristics of the system, system interfaces (internal and external), and the security and privacy controls to be deployed over the system, including controls inherited from IOT and/or the vendor hosting the system. Even off-the-shelf applications are to have a SSP prepared Authorization by a system owner that an information system is ready to operate, and process information indicates that the system owner accepts the residual risk of running the information system described in the SSP.

### FSSA Planning Standards

1. The system owner is responsible to prepare the System Security Plan for the application and its supporting infrastructure. The plan is to be distributed to the FSSA Privacy & Security Officer and other stakeholders identified by the system owner. The SSP is to be reviewed annually by the system owner for continued applicability and reviewed/updated whenever there is substantive change to the application, supporting infrastructure, security controls, or threat/risk profile (reviews/updates are to be documented in the SSP).
2. FSSA system security plans shall at a minimum include the following:
  - a. A title page, document history (reviews and update table with date, purpose, and reviewer identified) and an updated table of contents which correspond to the respective system of interest.
  - b. An introduction that includes the suggested audience, the information system security categorization, the contact information for the system owner and key contacts.
  - c. An enumeration of any confidentiality requirements relevant to the data created by, passing through or stored in the system.
  - d. A description of the operational environment for the information system including hardware, software, firmware, middleware/mobile code, and (if appropriate) networking/telecommunications equipment. The description must reflect any environmental or technical factors that are of security significance.
  - e. A detailed list of the interconnections with other internal and external information systems, including applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high-level design).
  - f. A description of the business process(es) that the information system supports, including user types and locations.
  - g. If the information system application(s) is hosted by a vendor, a copy of the vendor's FedRAMP certification and SOC II report.
  - h. A list of applicable laws and regulations to which the information system is subject (e.g., IRS Publication 1075, CMS MARS-E, SSA TSSR, HIPAA, HHS ACR OCSE, 7 CFR 272.1(c)).
  - i. Applicable rules of behavior (e.g., IRUA, agency or division specific)
  - j. Security and Privacy controls: each control family from the MARS-E baseline is to be addressed with respect to how the control is implemented, inherited, shared, or not applicable. Note: while most physical and environmental controls will be inherited either from IOT (for IOT-hosted applications) or the vendor (for vendor-hosted applications), the physical and environmental security controls for facilities, as applicable, should be addressed.
3. Security-related activities shall be planned and coordinated with other agency divisions, as applicable, to reduce the impact on organizational operations, assets, and users. Security-related activities include, for example, security assessments, audits, table-top simulations, system hardware and software maintenance, and contingency plan testing.

4. FSSA System Security Plans may reference other key security-related documents for the information system such as risk assessments, plans of action and milestones, any applicable privacy impact assessments, system contingency plan, checklists, or system interconnection agreements as appropriate.

# Section 13: Information Technology Risk Management Policy

### ***Purpose***

The purpose of this policy is to establish the IT risk management methodology and processes. Assessing and evaluating risk to information systems is critical to ensuring the confidentiality, integrity and availability of FSSA and FSSA client data.

The Information Security Risk Assessment (ISRA) incorporates the results of the Security Assessment and continuous monitoring controls to help make an overall determination of risk regarding the application and its supporting infrastructure, including the identification and acceptance of residual risk (the risk that remains after the successful application of the defined security and privacy controls). The ISRA may be incorporated into the SSP or be prepared as a separate document.

NIST Special Publication 800-30 R1 provides particular guidance in performing a risk assessment.

### ***Scope***

This policy applies directly to FSSA hosted information systems that store, process, and/or transmit CPI. Any FSSA business units who manage information systems that contain CPI are required to complete period risk assessments of these systems. Vendors who host FSSA information systems are required to have a substantially similar policy in place throughout the length of their contract. The FSSA Privacy & Security Office should be consulted to assist in determining the appropriate methodology, based on the size and complexity of the information system(s), for completing the required risk assessments.

### ***Risk Assessment Tool***

The determination of risk is the analysis of likelihood—how likely is it that the vulnerability/threat/weakness identified may be realized—and impact—if the vulnerability/threat/weakness is realized, what is the impact on operations, assets, individuals, or the organization?

		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood ↑	Very Likely	Low Med	Medium	Med Hi	High	High
	Likely	Low	Low Med	Medium	Med Hi	High
	Possible	Low	Low Med	Medium	Med Hi	Med Hi
	Unlikely	Low	Low Med	Low Med	Medium	Med Hi
	Very Unlikely	Low	Low	Low Med	Medium	Medium

### ***Risk Assessment***

It is the responsibility of the system owner to perform the risk assessment for the owner's applications and supporting infrastructure.

### ***Information Gathering***

Information used in an ISRA should be based on a current and detailed knowledge of the business unit's operating and business environments, security assessment, threat identification, continuous monitoring controls results. Both, technical and non-technical information should be gathered, including but not limited to network maps, review of controls, hardware/software inventories, as well as configurations, policies, standards, procedures for the operations, maintenance, upgrading, monitoring, physical security etc.

### ***Classify and Rank Sensitive Data, Systems, and Applications***

The criticality of the application and supporting infrastructure is determined following IOT's data classification procedures.

### ***Risk Analysis and Identification***

The risk analysis should address the following:

- Assumptions and constraints
- Threat sources (capability, intent, adversarial and non-adversarial)
- Threat events (sources, relevance, types)
- Vulnerabilities and predisposing conditions (affect likelihood of threat events occurring)

- Likelihood (how likely are threat events of concern going to result in adverse impacts?)
- Impacts (the degree of harm should a threat event occur—operations, assets, individuals, other organizations, the state
  - Vulnerabilities identified
  - Susceptibility of the safeguards (controls) planned or implemented to impede such events
- Categorize the risk (impact and likelihood)

### Risk Determination and Management

Based on the analysis, the determination of risk, which may be quantitative or qualitative, should be documented in the ISRA, identifying those risks that are acceptable and those that require additional safeguards/countermeasures to be employed. The latter should result in a POA&M to employ additional safeguards/countermeasures; for the former, the residual risk should be identified and accepted.

Risk mitigation strategies include:

- Risk Reduction. Actions taken to lessen the likelihood and/or adverse impacts associated with risk.
- Risk Avoidance. Decision not to become involved in, or action to withdraw from, a risk situation.
- Risk Transfer. Sharing with another party the burden of loss or benefit of gain, for a risk.
- Risk Retention. Acceptance of the burden of loss or benefit of gain from a particular risk.

The objective is to help ensure that the benefit of risk reduction outweighs the cost of the safeguards and countermeasures employed. As noted, this could be a qualitative determination (e.g., reputational risk is hard to quantify) or a quantitative determination (the likely cost of impact is lower than the cost of employing the appropriate safeguards).

### Monitoring and Review of Risk Assessment

The ISRA is to be reviewed annually by the system owner for continued applicability and reviewed/updated whenever there is a substantive change to the application, supporting infrastructure, or threat/risk profile, including the identification of new threats, threat vectors, and threat actors.

The system owner will submit the ISRA to the FSSA Privacy & Security Officer for review. The FSSA Privacy & Security Officer, in collaboration with FSSA management, may override the system owner's determination and acceptance of certain risks based on an enterprise view.

### Artificial Intelligence (AI) Risk Management Framework

In addition to any relevant security requirements identified in this policy, FSSA business units and/or contractors who implement or utilize any AI systems, shall provide evidence that these systems are being operated in accordance with the NIST AI Risk Management Framework 1.0 or later standard. Any alternate standards shall be approved by the FSSA Privacy & Security Office. Any implementation or use of an AI technology must be approved by the FSSA Privacy & Security Office, the Indiana Office of Technology, and the Office of the Chief Data Officer (OCDO) prior to the implementation or use the technology.

## Section 14: Definitions

These definitions apply to these Information Security Policies.

Term	Definition
Access Control(s)	The rules and deployment mechanisms which control physical and logical access to information systems are known as access controls. Access controls protect things perceived to be of value.
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.
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.
Anonymous account	An anonymous account is equal to a public or guest user which has no known affiliation with the agency or identifiable distinction.
Application	An application is composed of one or more pieces of computer programs. Applications may perform functions in an automated fashion using clearly defined rules to facilitate business goals and meet objectives. Applications require special consideration due to the sensitivity of the information they create, manipulate, maintain, or transmit.
AI Implementation Activities	Means the planning, design, development, deployment, operation, and monitoring, whether occurring independently or collectively, associated with an AI System.



AI System	Means an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI Systems are designed to operate with varying levels of autonomy.
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.
Authentication	Authentication is the process of verifying the claimed identity of a user. Authentication information should be kept confidential. Authentication is often discussed in terms of the three factors of authentication: something that is known to the individual; something that the individual has; and something that the individual is.
Authorization	A formal administrative approval required for an individual to gain access to a facility, system, or other information asset is known as authorization.
Availability	Availability is defined as ensuring timely and reliable access to and use of information. A loss of Availability is the disruption of access to or use of information or an information system [44 U.S.C., SEC. 3542].
Baseline Configuration	A baseline configuration is a documented, up-to-date specification to which the information system is built. It provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

Basic System User	An individual that is responsible for complying with all security requirements in order to obtain fundamental and primary access to an information system.
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.
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.
Confidentiality	Confidentiality is defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information [44 U.S.C., Sec. 3542].
Configurable devices	Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.
Configuration settings	Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system.
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 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.

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.
CVSS	The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. It was developed by a coalition of security professionals from around the world representing the commercial, non-commercial, and academic sectors. CVSS is used commonly to prioritize vulnerability remediation activities and calculate a score which communicates the overall severity of vulnerability discovered on one's systems.
Data Confidentiality Categories	As per the IOT data characterization reference, there are four confidentiality categories: confidential, sensitive, private and public. The implementation and execution of security safeguards and controls for applications varies depending on the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to information.
Emergency account	An emergency account is short term account that exists temporarily for a period of less than twenty-four (24) hours.
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.
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.
Federal Tax Information (FTI)	Federal Tax Information (FTI) is any tax return-derived information received from the Internal Revenue Service.

Identification	Identification is the process whereby a network element recognizes a valid user's identity. A user may be a person, a process, or a system (e.g., an operations system or another network element) that accesses a network element to perform tasks or process a call. Information used to verify the claimed identity of a user can be based on a password, Personal Identification Number (PIN), smart card, biometrics, token, exchange of keys, etc.
Identifier	An identifier is a name, label, code or symbol that labels the identity of an individual, device or object.
Information asset	An information asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and data. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the agency.
Information system and component inventory	Characteristics of an acceptable inventory of information system components are: accurate with respect to current configuration; sufficiently granular for tracking and reporting purposes; consistent with the authorization boundary of the system; enumerates manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.
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.
Information system security categorization	System security categorization relies upon the identification of the types of information stored or created within a system and determining the expected impact from a loss in confidentiality, integrity, and availability. An impact level of low, medium or high is determined for each type of information stored or created within a system. The overall impact level for the system is based on these impact levels for confidentiality, integrity, and availability.
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.

Integrity	Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information [44 U.S.C., Sec. 3542].
Internal networks	Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the State of Indiana.
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
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.
Least privilege	Assigning a user account only the most minimal rights required to access only the information and resources that are necessary to that user's work.
Local access	Local access is any access to an information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network.
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.
Logical Access Controls	Logical access controls are most often associated with login credentials procedures that grant or deny individuals the ability to read, write, or execute records or data contained in the information system.
Malicious code	Malicious code is computer code, software or programs that cause security breaches or damage to information systems. This includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats, contained within compressed files and is found on many forms of media such as USB devices, diskettes, or compact disks.
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.
National Vulnerability Database	The NVD is the U.S. government repository of standards-based vulnerability management data. This repository includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics
Network access	Network access is any access to an information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection.
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.
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.
Physical Access Controls	The ability to access areas or premises where information systems and technology assets reside depends on physical access controls. Physical access controls can be as basic as a locked door or as sophisticated as anti-pass-back mechanisms and man trap areas.

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.
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.
Privileged system user	An individual that is responsible for complying with all security requirements in order to obtain access to an information system. Privileged users (e.g. root or administrator) have a unique role within an organization as they are granted rights within the computer system which are significantly greater than those available to the basic system users.
Programming languages	Languages are formatted instructions, words, phrases or symbols that are read and translated into machine code so that a computer may execute them. Examples of programming languages are C, C++, Java, or C#.
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.
RBAC	Role-based access control provides a level of abstraction to establish permissions based on functional roles. Access decisions to systems and data are based on the role a user may have in the organization or information system. Roles may represent a task, position, responsibility or function assumed by an individual in a system.

Remote access	Remote access is a type of network access which allows an organization's users to access its nonpublic computing resources from locations other than the organization's facilities and often involves communication through an external network (e.g., the Internet).
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.
Residual Risk	The threat a risk poses after considering the current mitigation activities in place to address it and can be an important metric for assessing overall risk appetite.
Risk	Combination of the probability of an event and its consequence. The probable frequency and probable magnitude of future loss.
Risk Appetite	High level statement that broadly considers the levels of risk that management deems acceptable.
Risk Mitigation	The strategy to prepare for and lessen the effects of threats faced by FSSA. Mitigation is used to address deficiencies and to bring them to an acceptable risk tolerance. Risk Mitigation is also used in remediation activities.
Rules of behavior	The specifications and conditions users agree to follow as part of interacting with or using an information system are known as rules of behavior. Rules over behavior cover topics such as connection limits, remote access, information usage, assignment of system privileges and consequences for inappropriate behaviors.
Secure code standards	Secure code standards are specific rules and guidelines that document correct utilization of programming languages. These recommendations for building reliable secure programs when employed by developers minimize the number of vulnerabilities produced in the code at the time of the standard's publication.



Secure configuration	Recognized, standardized, and established benchmarks that stipulate secure configuration settings are developed by a variety of organizations including manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. These secure configuration settings are applied to information assets by following specific instructions pertinent to the respective information technology platform and product. Once the settings are applied and validated, the asset may be considered to be in a secure configuration.
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.
Security functions	Security functions such as authenticating, auditing, encrypting, and authorizing are deployed in hardware, software or firmware.
Security objectives	The three (3) most common security objectives considered for data and information systems are confidentiality, integrity and availability.
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.
System security plan	A system security plan delineates the responsibilities and expected behavior of all individuals who access an information system. It is documentation of the structured process for planning adequate, cost-effective security protection for a major application or information system.
Temporary account	A temporary account is an account that provides access for a limited duration to a system. Such an account may be granted to a user who may not have a long term affiliation with an agency. These accounts are often intended to expire within three-hundred-sixty-five (365) days.
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.
User account	A user account allows a user to authenticate to an information system services and be granted access. A person who uses a computer system has a user account. A user account is identified by a username or login name.

User account	A user account allows a user to authenticate to an information system services and be granted access. A person who uses a computer system has a user account. A user account is identified by a username or login name.
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Section 15: Policy Administration

### *Updates and Version Control*

Version	Revision Date	Revision Purpose	Completed By
1.0--Draft	November 2, 2020	Combined all previous Application Security Policies from 2014 into one document. Updated to include MARS-E 2.0 requirements. Initial Release for Comment.	Jordan Lake
1.0	March 5, 2021	Final version incorporating feedback from the Comment Period	Cliff McCullough
2.0	January 31, 2024	Added minor revisions to address federal audit findings.	Cliff McCullough
3.0	January 3, 2025	Added AI policy. Updated vulnerability remediation timelines.	Ahren Owen & Cliff McCullough

### *Annual Review*


These FSSA Information Security Policies are to be reviewed no less than annually by the FSSA Privacy and Security Officer to identify and make any needed updates. The FSSA Privacy & Security Officer will maintain a log of this annual review. Additionally, the *FSSA Policy Matrix* is used to track policy information at a granular level.

## Section 16: Signature Page

**Related Policies:** Replaces existing FSSA IS Policies and are combined in this document.


**Originating Office:** FSSA Privacy & Security Office

**Effective Date:** March 5, 2021

**Approval:**   
\_\_\_\_\_ on: January 27, 2021


Dr. Jennifer Sullivan, Secretary Date

**Effective Date:** January 31, 2024

**Approval:**   
\_\_\_\_\_ on: November 27, 2023

Daniel Rusyniak, M.D. Secretary Date

**Effective Date:** January 3, 2025

**Approval:**   
\_\_\_\_\_ on: November 7, 2024

Daniel Rusyniak, M.D. Secretary Date