



Family & Social Services Administration

Privacy & Security Compliance Policies & Procedures

Version 9.0

Effective: January 2, 2026

Contents

Introduction—Privacy & Security Compliance Policies.....	1
Section 1: Use and Disclosure Policy.....	2
Section 2: FSSA Privacy & Security Office	8
Section 3: Business Unit Privacy Policies & Procedures.....	10
Section 4: Privacy/Security Liaisons.....	12
Section 5: Incident Management & Breach Reporting Policy.....	14
Purpose	14
Policy.....	15
Section 5.1: Central Response and Reporting Management.....	16
Section 5.2: Privacy/Security Incident Staff Notification Requirements	18
Section 5.3: Privacy/Security Incident Investigation.....	21
Section 5.4: Privacy/Security Incident Determination.....	25
Section 5.5: Breach & Incident Notification.....	29
Section 5.6: Mitigation & Corrective Actions.....	32
Section 5.7: Notice to HHS	37
Section 5.8: Notice to Other Federal Agencies	39
Section 6: Email Policy	40
Section 6.1: Email Rules	41
Section 6.2: Email Security	44
Section 6.3: Using a Scanner to Scan/Send Client Personal Information	46
Section 7: Laptop & Portable Device Policy	47
Section 8: Fax Policy Section	55
Section 9: Computer & Paper & Media Disposal	58
Section 10: Training Requirements.....	60
Section 11: Staff Protection from Retaliatory Acts	65
Section 12: Sanctions for Policy Violation.....	66
Section 13: Retention Policy	67
Section 14: Federal Tax Information Background Checks	68
Section 15: Additional Privacy & Security Compliance Policies	72
Purpose	72

FSSA Privacy & Security Compliance Policies & Procedures

Policies	72
Section 16: Definitions	76
Section 17: Citations & Authorities	88
Section 18: Policy Administration	89

Introduction—Privacy & Security Compliance Policies

Purpose

The purpose of these Privacy & Security Compliance Policies and Procedures is to establish the rules and procedures to be followed by the Family & Social Services Administration (FSSA) and its personnel to ensure the confidentiality, security, and integrity of a client's personal information in FSSA's safekeeping.

Application

These Privacy & Security Compliance Policies apply to all FSSA divisions, bureaus, sections, facilities (including State Operated Facilities, or SOF's), 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 Privacy & Security Compliance Policies and Procedures are available to all FSSA personnel and other stakeholders on [The Hub website](#). Updated versions of these Policies and Procedures, made in accordance with Section 18, will be posted to *The Hub* within five (5) business days of final approval of the updates.

Section 1: Use and Disclosure Policy

Purpose

This policy establishes FSSA's general use and disclosure policy regarding all client personal information in FSSA's safekeeping.

Policy

FSSA staff may only access, use, and disclose client personal information as authorized and permitted by the applicable business unit's policies and procedures. Any access to, use of, or disclosure of client personal information not authorized or permitted by such policies and procedures is strictly prohibited and constitutes a violation of these Privacy & Security Compliance Policies.

A. FSSA staff may not disclose a client's personal information to anyone except to:

1. The individual to whom the personal information belongs.
 - 1.1. The individual has a right to see and get a copy of their client personal information.
2. The individual's Authorized Representative as identified in the individual's case file and subject to any limitations identified in the case file (e.g., the individual may have indicated that their Authorized Representative may only receive notices on their behalf).
3. The individual's parent or legal guardian if the individual is an unemancipated minor.
4. The individual's parent or legal guardian if the individual is a dependent adult and such is indicated in their file.
5. The individual's designated agent under a valid power-of-attorney, subject to the limitations, if any, in the power-of-attorney.
6. Persons or organizations authorized in writing by the individual to receive their client personal information:
 - 6.1. A signed and valid authorization form must be on file for the individual.
 - 6.2. The types of client personal information that may be disclosed under the authorization must be limited to the client personal information so identified on the authorization form.
 - 6.3. Each division and business unit has an authorization form in place specific to that division or business unit. The appropriate form applicable to the division or business unit is the form that must be signed by the individual in order for the division/business unit to disclose the client personal information.
7. Co-workers who are authorized by the business unit's policies to see and use the client personal information.
8. Other FSSA business units that have a lawful purpose to see and use the client personal information, as defined in the originating business unit's policies; such disclosures may be subject to a valid Memorandum of Understanding between the business units.

9. Other state agencies that have a lawful purpose to see and use the client personal information, as defined in the originating business unit's policies and subject to a valid Memorandum of Understanding between FSSA and the other state agency being in place.
 - 9.1. Client personal information may not be disclosed to other state agencies absent a valid Memorandum of Understanding being in place; other state agencies are not necessarily covered under the same federal and state laws and regulations as FSSA.
10. Contractors that are authorized to see and use the client personal information on FSSA's behalf, subject to a written agreement with FSSA that contains the applicable privacy and security safeguards (including the necessary Business Associate language for contractors permitted to see and use PHI) and that permits the use/disclosure. The terms of the agreement must be approved by the FSSA Privacy & Security Officer.
11. Providers who provide services to FSSA clients and have a direct treatment relationship with the individual (e.g., physicians, hospitals, mental health centers, physical therapists, etc.).
 - 11.1. If there is no existing or anticipated direct treatment relationship in place, client personal information cannot be disclosed to a provider simply because they are a provider.
 - 11.2. Note that minimum necessary does not apply with respect to disclosing client medical information and benefits coverage to providers that have a direct treatment relationship with the client.
12. Legitimate research organizations subject to a valid Research Data Sharing Agreement between FSSA and the research organization that includes the appropriate Institutional Review Board documents.
13. The FSSA Privacy & Security Officer as may be necessary to investigate and manage improper disclosures of client personal information.
14. As otherwise required by law and permitted under the applicable state and federal regulations.
 - 14.1. The FSSA Privacy & Security Officer can provide guidance regarding other permitted disclosures.
- B. **Disclosures for legislative inquiries:** Disclosures of any client personal information to Legislators or their staff requires the completion of the "AUTHORIZATION TO ACT ON CONSTITUENT'S Behalf Form" (State Form 54530) and signed by the client or their personal representative. Any alternate authorization forms must be approved by the FSSA Privacy & Security Officer prior to the disclosure.
- C. **Minimum Necessary:** All uses and disclosures of client personal information by FSSA, including FSSA's own use of client personal information, will be limited to the minimum information necessary to fulfill the purpose of the use or disclosure as defined in the business unit's policies, with the exception of disclosures to the individual or others as identified within federal law.
- D. **Collection, Use, Retention, Disposal:** In concert with the Minimum Necessary policy, FSSA business units are responsible to assure that business processes and supporting computer systems are designed to minimize the collection and use of client personal information to the extent possible. This includes, but is not limited to:

- a. Identifying the minimum client personal information necessary for each business process and computer system (relevant and necessary to accomplish the legally authorized purpose of the collection and use);
- b. Limiting the client personal information collected to the elements identified and annually reviewing the collection/use to assure that it remains necessary;
- c. Where possible, remove/redact, anonymize, and/or de-identify client personal information held by the business unit to reduce risk of improper disclosure;
- d. Retain client personal information, whether electronic or otherwise, for only the minimum time required by law or regulation;
- e. Where possible, archive client personal information that needs to be retained, but is no longer needed for routine business purposes off primary computer systems to reduce the risk of improper disclosure;
- f. When client personal information no longer needs to be retained, dispose of the information in a manner that prevents loss, theft, misuse, or unauthorized access (i.e., assuring secure deletion or destruction).

E. Role-based Access: Each business unit is responsible under FSSA's Access Control Policy to establish and document Role-based Access profiles identifying the proper level of personnel access to client personal information, whether electronic or otherwise, commensurate with staff roles and responsibilities, including contractor roles and responsibilities; such Role-based Access profiles will be designed to assure that only the Minimum Necessary amount of client personal information is provided to each role and all roles incorporate the principle of least privilege. It is the responsibility of the business unit to validate that the Role-based Access profiles are in compliance with all applicable federal and state laws and regulations, including verification that any relevant access agreements are signed, documented appropriately, and adhered to by its personnel.

Intentionally accessing client personal information without a lawful business need is a direct violation of these policies and will result in appropriate discipline action. This includes, but not limited to, accessing the records of family, friends, neighbors, co-workers, and/or celebrities.

F. Verification: When a client or their representative calls-in we are required by federal regulations to verify their identity before disclosing any client personal information. Have them tell you¹:

1. Case Number or Person ID
2. Client's full name
3. Client's date of birth
4. Last four digits of the client's Social Security Number
5. If a representative is calling:
 - a. If it is an Authorized Representative, be sure a valid AR form is on file
 - b. If it is a parent or guardian:

¹ A business unit may require alternative identity verification procedures based on the unit's requirements.

- i. For unemancipated minors, they are the legal parent (rights have not been terminated) or guardian as identified in the case file;
- ii. For dependent adults, they are the legal parent or guardian as identified in the case file.
- c. If another type of representative (e.g., have power-of-attorney, the client's attorney, etc.), that supporting documentation is in the case file.

If there is any doubt about the client's identity, ask for additional identifying information (e.g., full SSN, complete address, etc.).

If you are on the phone with a client or in a face-to-face interview and there are others on the call or at the interview (who are not verified as the client's Authorized Representative or parent/guardian), obtain the client's verbal permission to discuss the client's personal information in front of the others and document that permission in the case notes.

- G. Additional Restrictions:** Disclosure of certain client personal information may be further limited under applicable business unit policy (e.g., the Division of Mental Health & Addiction has more restrictive disclosure policies for certain members of its service population) and other FSSA policies.
- H. Individual Responsibility:** It is each FSSA staff member's responsibility to ensure that client personal information is only used and disclosed in accordance with this policy and in accordance with the staff member's business unit's policy. When in doubt, ask your supervisor for guidance and/or seek clarification with the FSSA Privacy & Security Officer.
- I. No personal use:** It is a **direct violation of this policy for a FSSA staff member to use any client personal information in FSSA's safekeeping for personal reasons or personal gain. You are prohibited from accessing any FSSA client personal information regarding yourself, your family, your co-workers, your friends, or business associates.** In addition, any use of client personal information in FSSA's safekeeping for a staff member's personal reasons or personal gain may subject the staff person to significant civil and criminal penalties under state and federal law, as well as sanctions under FSSA and state policy.
- J. Social Media:** At no time may a FSSA staff member post any client personal information or make any references to clients on any social media account or page, including but not limited to Internet forums, web-blogs, social blogs, micro blogs, wikis, podcasts, photo pages, and other permutations. Examples of social media include, but are certainly not limited to Facebook, Twitter, LinkedIn, Instagram, Pinterest, Tumblr, Snapchat, Flickr, Reddit, WhatsApp, Google+, Yelp, Yammer, and YouTube.
- Doing so is a **direct violation of these Privacy & Security Compliance Policies** and may subject the staff member to sanctions in accordance with state and FSSA policy, as well as criminal and civil penalties. The only exception to this policy would be a situation where an FSSA client has provided written authorization that specifically authorizes the FSSA Office of Communications to post information to social media (e.g., highlighting an FSSA client success story).
- K. Social Security Number Uses:** All FSSA business units shall keep the use and/or disclosure of a Social Security number to the minimum necessary to complete the lawfully authorized activity. If an

individual's Social Security number is necessary for a lawfully authorized activity, the FSSA business unit shall initially review the activity to determine if using only the last four (4) digits will suffice for the activity. In all cases, the FSSA business units shall employ an appropriate encryption method that meets or exceeds the FSSA encryption standards for electronic uses of Social Security numbers (i.e., data at rest, data in transit, and data in use). All paper documents containing Social Security numbers shall be properly secured at all times and then disposed of in accordance with these policies when no longer needed.

- L. **Training Materials, Policy Documents, and Other Guidance:** Client personal information is **prohibited from being used** in any training materials, policy and procedure documents, provider and user guides, training web pages or applications, or other guidance materials prepared by a FSSA division/business unit. This includes examples and any other permutations in which client personal information is presented or displayed. Exceptions to this policy require written permission of the FSSA Privacy & Security Officer.
- M. **Test Data:** Client personal information is **prohibited from being used** for information system testing under any scenario or condition. Exceptions to this policy require written permission and risk acceptance by the applicable Division Director and written concurrence by the FSSA Privacy & Security Officer.
- N. **Output Devices:** Access to output devices such as printers, fax machines, multi-function devices, and similar output devices are to be physically secured to minimize the risk of inadvertent, unauthorized disclosure of client personal information. Physical security may include the use of passwords and PIN codes that prevent the output from printing until entered on the device by the user (user must be physically present to enter the code and receive the output).
- O. **Computer Workstations:** Workforce member computer workstations are to be locked (requiring entry of a password to access) whenever the workforce member will leave the workstation unattended. Computer monitors should be positioned to minimize viewing by others.
- P. **Clean Desk:** At the end of the work day and when FSSA personnel will be away from their work area for a sustained period (e.g., vacation), FSSA personnel are to clear their work area of any materials that contain client personal information and place such materials in a locked drawer or filing cabinet. During shorter periods, such as a lunch break, FSSA personnel should clear, cover, or otherwise conceal any materials in their work area that contain client personal information.
- Q. **Screen Prints:** FSSA personnel are prohibited from printing (via screen print or similar means), photographing, video recording, or otherwise recording/reproducing computer screens that contain client personal information unless authorized by the individual's supervisor or division director/business unit head for a particular purpose (e.g., troubleshooting a problem, recording an application issue). If so authorized, once the purpose has been accomplished the reproduction will be destroyed so that it cannot be read or used or recreated.
- R. **Password Security:** Passwords must be kept private and secure. A workforce member sharing their password is a violation of these policies and procedures and the workforce member will be held accountable for any actions taken by anyone with whom they shared their password. If a password

is inadvertently compromised, the workforce member will immediately change their password and report it to the IOT Help Desk. In addition, workforce members are to logoff of their workstation before allowing anyone else to use it—not logging off is the same as sharing the password.

Guidance: The FSSA Privacy & Security Officer can provide additional guidance on use and disclosure rules.

Procedures

Each FSSA business unit will develop/update its policies and procedures to further identify permitted and not permitted uses and disclosures of client personal information, including applicable minimum necessary provisions.

Section 2: FSSA Privacy & Security Office

Purpose

It is a regulatory requirement (reference §164.530(a)(1)(i) of the HIPAA Privacy Rule) that FSSA designate a Privacy & Security Officer responsible for the development and implementation of the privacy policies and procedures of the agency. The establishment of a Privacy & Security Officer (or official) also meets the requirements of the AR-1 privacy controls under MARS-E, with which certain FSSA business units (e.g., DFR) must comply.

Policy

FSSA shall designate a Privacy & Security Officer (also referred to as the HIPAA Compliance Officer) responsible for the development, implementation, and maintenance of the agency's privacy and security policies and procedures, and assuring FSSA's ongoing compliance with the various federal and state privacy laws and regulations applicable to FSSA. The FSSA Privacy & Security Officer will review the FSSA Privacy & Security Compliance Policies & Procedures and the FSSA Security Policies within every 365 days and make any necessary updates; whether or not any updates are made, the FSSA Privacy & Security Officer will record his/her review in a cumulative review log established for this purpose.

The FSSA Privacy & Security Officer is in-charge of and responsible for the FSSA Privacy & Security Office, including any staff assigned to the Privacy Office. The Privacy & Security Officer may delegate certain responsibilities and authorities to Privacy & Security Office staff, at his or her sole discretion.

The FSSA Privacy & Security Officer is responsible for and is authorized to oversee, direct, and control the agency's response, in collaboration with FSSA management, to any and all known or suspected privacy/security incidents, including the associated actions of contractors involved in any such privacy/security incidents.

The FSSA Privacy & Security Officer shall serve as the agency's primary point of contact regarding privacy complaints, incident response/reporting, and similar interactions with the US Department of Health and Human Services/Office of Civil Rights, the Social Security Administration, the Internal Revenue Service, the HHS/Office of Child Support Enforcement, the Centers for Medicare & Medicaid Services, and the Indiana Attorney General's Office. The FSSA Privacy & Security Officer shall also serve as the agency's primary point of contact regarding vendor/contractor notifications to FSSA of known or suspected security and/or privacy incidents, and similar items.

The FSSA Privacy & Security Officer is responsible for the development, implementation, and maintenance of the agency's privacy program and plan, including the agency's risk management plan. The FSSA Privacy & Security Officer may direct individual business units to conduct periodic risk assessments.

The FSSA Privacy & Security Officer shall collaborate with FSSA management, including division management, on the development and implementation of Business Unit Privacy Policies & Procedures (reference Section 3), the appointment of Privacy/Security Liaisons (reference Section 4), and other privacy and security matters.

FSSA Privacy & Security Compliance Policies & Procedures

The FSSA Privacy & Security Officer is responsible for the development, implementation, and maintenance of the agency-wide security policies. The FSSA Privacy & Security Officer will coordinate with the Indiana Office of Technology (IOT) and the FSSA Division of Technology Services (DTS) for implementation of any required technical standards. The FSSA Privacy & Security Officer's other responsibilities are identified throughout these Privacy & Security Compliance Policies.

Procedures

The FSSA Privacy & Security Officer will prepare procedures applicable to the Privacy & Security Officer's duties and responsibilities as identified throughout these Privacy & Security Compliance Policies.

Section 3: Business Unit Privacy Policies & Procedures

Purpose

These Privacy & Security Compliance Policies and Procedures apply to all FSSA divisions, bureaus, sections, facilities, and program areas (collectively and individually, “business units”) and all FSSA personnel.

The agency-wide policies also provide a framework for the development and promulgation of policies and procedures by and unique to each business unit. The purpose of this policy and its supporting procedures is to establish the requirement that all FSSA business units are responsible to develop and promulgate subsidiary privacy policies and procedures that are unique to the needs of the business unit.

Policy

Each business unit will establish subsidiary privacy policies and procedures that are unique to the needs of the business unit, reflecting the unit’s business procedures and interactions with individual clients and incorporating, as necessary, federal or state laws and regulations specifically applicable to the business unit.

FSSA business units may establish privacy policies and procedures that are more restrictive than these Privacy & Security Compliance Policies; and, in certain cases, may be obligated to do so under federal or state laws and regulations specifically applicable to the business unit.

However, in no case may a business unit establish privacy policies and procedures that are less restrictive, contrary to, or otherwise circumvent these agency-level Privacy & Security Compliance Policies and Procedures without the express, written permission of the FSSA Privacy & Security Officer. Exceptions may be granted, but only where a solid business and legal case can be made for the exception.

Procedures

The following provides additional guidance for this policy.

1. Certain business units that are subsidiaries of a parent business unit may adopt the parent business unit’s privacy policies and procedures and not develop its own, provided the subsidiary does not have any privacy requirements that are unique to its business function. The parent business unit management team and the Privacy & Security Officer must approve these exceptions.
2. Business unit privacy policies and procedures are to be submitted to the Privacy & Security Officer for review and approval.
 - 2.1. The Privacy & Security Officer’s approval is limited to ensuring the privacy policies and procedures are not less restrictive, contrary to, or otherwise circumvent these Privacy & Security Compliance Policies and Procedures; are not contrary to applicable federal and state laws and regulations; and, meet generally accepted privacy best practices.
 - 2.2. The Privacy & Security Officer may make specific recommendations regarding business unit privacy policy and procedure content.
 - 2.3. The Privacy & Security Officer will maintain a central log of all business unit specific privacy policies and procedures.

3. Business unit privacy policies and procedures should be a supplement to these Privacy & Security Compliance Policies and Procedures. For example, a business unit may insert supplemental privacy policies and procedures (by way of links) into these Privacy & Security Compliance Policies and Procedures; or, provide a reverse cross-reference to these Privacy & Security Compliance Policies and Procedures within the business unit's privacy policies and procedures.
4. Business units should also consider integrating their privacy policies and procedures with other, relevant policies and procedures in order to provide a consolidated and uniform set of policies and procedures for their staff and business operations.
5. *Privacy Impact & Risk Assessment:*
 - 5.1. Each business unit is responsible to implement a privacy risk management process that assesses the risk to individuals resulting from the collection, storage, sharing, transmitting, use, and disposal of client personal information.
 - 5.2. In accordance with its privacy risk management process, each business unit is responsible to conduct privacy impact assessment for its information systems, programs, operations, and other activities that pose a risk to the privacy of client personal information.
 - 5.2.1. This assessment should be performed annually or whenever significant changes occur to the business unit's information systems, programs, or operations.
 - 5.2.2. This assessment should be performed in accordance with the IOT Tier 1 Security Standard IOT-CS-SEC-100, Risk Assessment Procedure, and employ other risk assessment procedures as deemed appropriate by the division director/business unit head.
 - 5.2.3. The results of the risk assessment are to be provided to the FSSA Privacy & Security Officer for review and comment.
6. Business units will review all relevant privacy and/or security policies every 365 days. If no substantive changes are necessary, a log of this review will be maintained by the business unit validating the date of the review. A copy of this log will also be submitted to the FSSA Privacy & Security Office on an annual basis.

Section 4: Privacy/Security Liaisons

Purpose

The purpose of this policy is to ensure each FSSA division, state operated facility, and business unit, as appropriate, has a designated staff member assigned to serve as the Privacy/Security Liaison for that division, state operated facility, or business unit.

The scale and scope of FSSA requires Privacy and Security coordination between the FSSA Privacy & Security Officer and the FSSA business units on a number of fronts, including, but not limited to, management of privacy/security incidents, business unit specific privacy and security policy and procedure development, and providing a knowledgeable resource to assist staff with privacy/security related questions and issues.

Policy

Each FSSA division will assign an appropriately qualified staff member to serve as the division's Privacy/Security Liaison. Each state operated facility (hospital) will assign an appropriately qualified staff member to serve as the facility's Privacy/Security Liaison.

At a minimum, each division and state operated facility will have a designated Privacy/Security Liaison. As determined by each division in collaboration with the FSSA Privacy & Security Officer, additional Privacy/Security Liaisons may be designated for the various bureaus, sections, program areas, and offices within the division. The Privacy/Security Liaisons will be responsible to:

1. Ensure all staff members within their assigned area are familiar with and understand FSSA's Privacy & Security Compliance policies and procedures.
2. Ensure all staff members within their assigned area complete any and all required privacy and security training as promulgated by the FSSA Privacy & Security Officer, including both initial and refresher training.
3. Develop and document privacy and security policies and procedures as applicable to their assigned area (as business unit-specific policies and procedures that are a subsidiary of FSSA's Privacy & Security Compliance Policies and Procedures, as described in Section 3), as directed by and in collaboration with division management.
4. Collaborate as necessary with the FSSA Privacy & Security Officer regarding the development of business unit-specific privacy and security policies and procedures.
5. Ensure all staff members within their assigned area are familiar with and understand any business unit-specific privacy policies and procedures and are trained on same.
6. Coordinate with the FSSA Privacy & Security Officer on privacy/security incidents as further described elsewhere in these Privacy & Security Compliance Policies (following the associated policies and procedures).
7. Report on their activities to the FSSA Privacy & Security Officer on a regular basis (as deemed necessary and appropriate by the FSSA Privacy & Security Officer).

8. Privacy/Security liaisons, including state employees and/or contractors who serve as Security Coordinators granting/facilitating access to agency applications containing any form of client personal information (CPI) are required to adhere to the following processes:
 - 8.1. Successful completion of a relevant background check.
 - 8.2. Verifying that each user has a lawful business need to the system. Understanding that they are directly accountable for verifying that only the proper access is requested.
 - 8.3. Verifying that each user is only granted access to the minimum necessary amount of CPI to meet the lawful business need.
 - 8.4. Agrees to participate in periodic reviews of account audit activity to validate ongoing access needs. Further, they agree to notify the FSSA Privacy & Security Office no later than one (1) business day of any staff who need to have their access terminated. If an emergency situation arises, they agree to submit a termination request immediately. They agree to follow the notification processes developed by the FSSA Privacy & Security Office.

Procedures

Each Privacy/Security Liaison will develop procedures pertinent to their assigned area designed to assure compliance with this policy.

Section 5: Incident Management & Breach Reporting Policy

Purpose

The purpose of this policy and its supporting procedures is to ensure the timely reporting of known or suspected security and privacy incidents so that appropriate action can be taken in a timely manner to prevent or mitigate any improper disclosures of [client](#) personal information.

This section comprises the incident reporting and response plan for FSSA.

This policy is organized into several sections with each focusing on a particular policy regarding Incident Management & Breach Reporting:

1. [Section 5.1:](#) Central Response and Reporting Management
2. [Section 5.2:](#) Privacy/Security Incident Staff Notification Requirements
3. [Section 5.3:](#) Privacy/Security Incident Investigation
4. [Section 5.4:](#) Privacy/Security Incident Determination
5. [Section 5.5:](#) Breach Notification
6. [Section 5.6:](#) Mitigation & Corrective Actions
7. [Section 5.7:](#) Notice to HHS
8. [Section 5.8:](#) Notice to Other Federal Agencies

One of the missions of the FSSA Privacy & Security Office is to manage all privacy and security incidents for FSSA, under the direction of the FSSA Privacy & Security Officer. The scope of this responsibility includes all agency personnel, divisions, offices, and facilities, as well as, centralized coordination with, as appropriate, agency management, FSSA Communications, FSSA General Counsel, FSSA Division of Strategy & Technology, the IOT Information Security Incident Response Team and the State CISO, law enforcement, the Indiana Attorney General's Office, applicable federal agencies, and others as deemed appropriate by the FSSA Privacy & Security Officer.

The objective is to assure that all privacy and security incidents are quickly identified and reported, contained, and corrective actions determined to prevent or mitigate similar incidents. Protecting the privacy of FSSA's clients is of the utmost importance.

The FSSA Privacy & Security Office has a dedicated incident response team that will be dynamically expanded at the direction of the FSSA Privacy & Security Officer to include other, appropriate resources (such as the IOT ISIRT) based on the nature of any particular privacy and security incident. Additional responsibilities and management requirements are addressed throughout the following policies and procedures.

This Section 5 Incident Management & Breach Reporting Policy will be reviewed annually as part of the FSSA Privacy & Security Compliance Policies and Procedures annual review process. Updates to this section will be made whenever necessary to enhance FSSA's incident response capability.

Policy

It is the agency's policy that all privacy/security incidents are to be reported to the FSSA Privacy & Security Officer, who will centrally manage FSSA's response to ensure response consistency, legal and regulatory compliance, and cost management. The FSSA Privacy & Security Officer, working appropriately with FSSA management, the affected business unit's management and Privacy/Security Liaison, and others as applicable, will investigate the incident, determine whether a breach has occurred, ensure appropriate mitigation and corrective action procedures are or will be undertaken, and provide or cause to provide appropriate notice when required.

Under Section 10, all FSSA workforce members will be trained on FSSA's Incident Management & Breach Reporting policy as part of the overall FSSA Privacy & Security Compliance Policies & Procedures training. In addition, the FSSA Privacy & Security Officer may provide additional training, including by way of on-the-job training, to FSSA personnel with specific incident response and reporting responsibilities.

FSSA's Incident Management & Breach Reporting policy and procedures will be integrated to the extent necessary and appropriate with the agency's Continuity of Operations Plan.

Section 5.1: Central Response and Reporting Management

Purpose

A timely and expert response to known or suspected privacy/security incidents is vital to managing and mitigating the impact of the incident, with the objective of taking immediate action to stop the incident if it is ongoing; and, to complete an appropriate and structured investigation into the cause and effect of the incident, including ascertaining the potential harm to the individuals (victims) subject to the incident and risk to the agency.

In addition, given the potentially significant costs involved in mitigation activities and providing notice to the victims (as may be required under federal and/or state law), the reporting requirements to the Office of the Indiana Attorney General and the applicable federal agencies (e.g., Department of Health and Human Services/Office of Civil Rights, Centers for Medicare and Medicaid Services, the Social Security Administration, the Internal Revenue Service, the HHS/Office of Child Support Enforcement, etc.) and the potential harm that may be caused by a substantive incident, it is appropriate to centralize management of the incident investigation and mitigation process (including notice). This helps assure a uniform approach, appropriate involvement by all applicable state agencies and departments in the process, and a streamlined notification and reporting process.

Policy

The FSSA Privacy & Security Officer will centrally manage all reported privacy/security incidents, both known and suspected. The Privacy & Security Officer will involve FSSA management, other FSSA divisions, state agencies, IOT, and law enforcement as appropriate and needed under the circumstances.

The FSSA Privacy & Security Officer is responsible for oversight, direction, and control of the incident investigation and may delegate, as appropriate under the circumstances, investigation and mitigation activities to other FSSA personnel, including contractors. Such personnel will cooperate with the FSSA Privacy & Security Officer and undertake those assigned activities in a timely and competent manner.

As designated by the FSSA Privacy & Security Officer, Privacy & Security Office staff may oversee, direct, and control privacy/security incident response procedures of behalf of the FSSA Privacy & Security Officer.

Procedures

The FSSA Privacy & Security Office has internal procedures in place to guide its response to reported privacy/security incidents, including incident risk determination and management procedures, documentation procedures, notice development and dissemination procedures, and communication procedures.

The FSSA Privacy & Security Office will integrate this policy with the relevant incident management procedures of the Indiana Office of Technology in accordance with IOT Tier 1 Security Standards IOT-CS-SEC-132 and 133.

The FSSA Privacy & Security Office will annually test the agency's incident response and reporting procedures through a checklist review of its performance with respect to actual incidents to identify

improvements and assure ongoing effectiveness. This review will be documented by means of the completed checklist that will be retained by the FSSA Privacy & Security Officer.

These procedures will include reporting of incidents to the appropriate federal agencies as determined by the type of information that is or may be subject to a privacy/security incident, including but not limited to the Internal Revenue Service and/or the Social Security Administration for Federal Tax Information, the Social Security Administration for SSA data, the Centers for Medicare and Medicaid Services for PII received from the federal data services hub, and the HHS/Office of Child Support Enforcement for National Directory of New Hires (NDNH) data.

The procedures for incident reporting predominately rely on the use of email or phone or in-person reporting. In the event that one or more of those methods are compromised (e.g., malware that has infected the email system) and cannot be relied upon, the FSSA Privacy & Security Officer will establish an alternative means of communication, in conjunction with the FSSA Office of Communications & Media and FSSA Facilities Management, based on the circumstances.

Section 5.2: Privacy/Security Incident Staff Notification Requirements

Purpose

The purpose of this policy and its supporting procedures is to ensure the timely notification of the appropriate Privacy/Security Liaison by FSSA personnel of a known or suspected privacy/security incident.

Policy

FSSA personnel will promptly notify their assigned Privacy/Security Liaison (PSL) should they learn of or reasonably suspect that a privacy/security incident has occurred. This notice should occur on the same business day that FSSA personnel become aware of the incident. This includes known or suspected privacy/security incidents reported to a staff member by clients and/or FSSA contractors.

Alert: If you suspect that your computer has been infected with a virus or other type of malware, or if you've accidentally opened a spam message, immediately contact the IOT Help Desk to report the issue, and then contact your PSL. A virus, if not removed, can cause extensive damage to state systems.

Advisory: FSSA personnel reporting known and suspected privacy/security incidents are protected from any recrimination or retaliatory acts under the state's and FSSA's whistleblower and retaliatory protection policies.

Failure to report a known or suspected privacy/security incident **is a violation of this policy** and may result in personnel sanctions in accordance with state and FSSA policy.

Procedures

1. FSSA personnel are to be on the alert for any known or suspected privacy/security incidents.

Advisory: FSSA prefers that its personnel err on the side of caution and report any suspected privacy/security incident—if you are unsure, contact your assigned PSL or supervisor for guidance. It is better to report an incident that, in the end, is not a privacy/security incident than to risk a real incident going unreported. And, no one will be reprimanded for doing so.

2. FSSA personnel are directed to promptly notify their assigned Privacy/Security Liaison of a known or suspected privacy/security incident.

2.1. Such notice should be in person, by phone, or by email.

Alert: If a Business Associate/Contractor contacts you and reports a privacy/security incident or breach, promptly contact the FSSA Privacy & Security Officer.

3. If the assigned PSL is not available, the staff person should then immediately notify both their supervisor² and the FSSA Privacy & Security Officer (at FSSA.PrivacyOffice@fssa.in.gov).

- 3.1. Such notice should be in person, by phone, or by email.
4. The staff person discovering the privacy/security incident should try to capture as much information about the incident as possible—write it down; however, don't delay notice just to capture this information:
 - 4.1. Date and time of when you discovered the incident.
 - 4.2. When the incident occurred (date and time), if known.
 - 4.3. How you discovered the incident.
 - 4.4. The nature of the incident:
 - 4.4.1. *What information* was disclosed or compromised (e.g., name, address, RID#, Case#, SSN, date of birth, medical record, etc.)?
 - 4.4.1.1. Obtain a copy of the information disclosed, if possible;
 - 4.4.2. *To whom* the information was disclosed?
 - 4.4.3. *The volume* of information disclosed (e.g., how many people, how many records, etc.);
 - 4.4.3.1. The names and addresses of the people affected (victims)—may require some investigation or provision of a file if a large number were affected;
 - 4.4.3.2. Which FSSA programs are the victim(s) enrolled in or applying for (e.g., Medicaid, a Waiver program, SNAP, TANF, etc.)?
 - 4.4.4. *How* the incident occurred.
 - 4.4.5. Whether ***Social Security Numbers*** were disclosed or compromised.
 - 4.4.6. *What actions* were taken to mitigate the incident (if any)?
 - 4.4.7. And, any other information that seems pertinent.
 - 4.5. To whom you reported the incident, include date, time, and method (e.g., in person, by phone).
 - 4.6. Your name and contact information.
5. The FSSA Privacy & Security Officer may contact the staff person for additional information, as needed.
6. If, for whatever reason, the staff person making the notification to the PSL believes that the PSL is not being responsive or timely, the staff person should contact the FSSA Privacy & Security Officer and report the privacy/security incident.

Advisory: Disclosures that occur incidental to the use or disclosure of client personal information otherwise permitted by these Privacy & Security Compliance Policies, *et seq*, may not constitute a

² If the supervisor is the one suspected of causing the privacy/security incident and the staff person is uncomfortable reporting the incident to this same supervisor, the staff person should directly notify the FSSA Privacy & Security Officer.

privacy/security incident, provided such use or disclosure is a by-product of a permissible use or disclosure, cannot be reasonably prevented, and is limited in nature. For example, an Eligibility Specialist's computer screen locks up while displaying client information; the IT person who fixes the problem likely will see the information; this is an incidental disclosure and not a violation or breach. Such incidental disclosures do not need to be reported as privacy/security incidents; when in doubt, seek guidance from your Privacy/Security Liaison or the FSSA Privacy & Security Officer.

Section 5.3: Privacy/Security Incident Investigation

Purpose

The purpose of this policy and its supporting procedures is to establish the requirements and general approach for the investigation of known and suspected privacy/security incidents as reported by FSSA personnel or as otherwise becomes known to FSSA.

Policy

The applicable FSSA Privacy/Security Liaison and the FSSA Privacy & Security Officer are responsible to promptly investigate any known or suspected privacy/security incidents.

Alert: If the incident involves the improper disclosure of (or possible disclosure of) an individual's Social Security Number, the incident must be reported to the Office of the Indiana Attorney General within two (2) business days of when the Social Security Number was disclosed³. The FSSA Privacy & Security Officer will provide any notifications to the OAG.

Procedures

1. The Privacy/Security Liaison⁴ **will begin a preliminary investigation** of a reported privacy/security incident on the same business day the incident was reported to the PSL by FSSA personnel or the same business day the PSL otherwise learned of a known or suspected privacy/security incident. The investigation should focus on collecting the facts and circumstances regarding the incident:
 - 1.1. Date and time of the privacy/security incident was discovered.
 - 1.2. *Who* (FSSA staff) reported the incident (name, title, contact information)?
 - 1.3. *How* was the incident discovered?
 - 1.4. The nature of the incident:
 - 1.4.1. *What information* was improperly disclosed or compromised (e.g., name, address, RID#, Case#, SSN, date of birth, medical record, etc.)?
 - 1.4.2. *To whom* the information was disclosed?
 - 6.1.1.1. *The volume* of information disclosed (e.g., how many people, how many records, etc.); The names and addresses of the people affected (victims)—may require some investigation or provision of a file if a large number were affected;
 - 6.1.1.2. Which FSSA programs are the victim(s) enrolled in or applying for (e.g., Medicaid, a Waiver program, SNAP, TANF, etc.)?
 - 1.4.3. *How* the incident occurred including the names, titles, and contact information of persons involved in the incident?

³ Reference IC 4-1-10 and 10 IAC 5-1-1.

⁴ If a PSL is not available, the PSL responsibilities outlined here become the responsibility of the supervisor or manager of the person who reported the privacy/security incident.

1.4.4. *Whether **Social Security Numbers** were improperly disclosed or compromised;*

Alert: If a Social Security Number(s) was disclosed or suspected to have been disclosed or otherwise compromised, the PSL is to notify the FSSA Privacy & Security Officer on the same business day so that the FSSA Privacy & Security Officer can provide a timely, even if preliminary, notice to the OAG.

1.4.5. *Whether **Federal Tax Information, Social Security Administration Information, or National Directory of New Hires Information** was improperly disclosed or compromised;*

Alert: Certain federal agencies provide information to FSSA via data exchanges. This includes Federal Tax Information (FTI) provided by both the Internal Revenue Service and the Social Security Administration; Social Security Administration Information provided by the Social Security Administration (SSA Data); National Directory of New Hires Information (NDNH Data) provided by the HHS Office of Child Support Enforcement; and, applicant/beneficiary information provided by the Centers for Medicare & Medicaid Services via the Federal Data Services Hub (CMS FDSH Data). If any of these data types was disclosed or suspected to have been disclosed or otherwise compromised, the PSL is to **immediately** notify the FSSA Privacy & Security Officer. In these situations, the agency is required to immediately report the incident to the appropriate federal agency (the report will be made by the FSSA Privacy & Security Officer).

1.4.6. *What actions have been taken to mitigate the incident (if any)?*

1.4.7. *And, any other information that seems pertinent.*

Advisory: Not all privacy/security incidents may involve the improper disclosure of client personal information, but rather may place the integrity of client personal information at risk. For example, a staff member changed a client's personal information on a computer system without authorization or with malicious intent. Therefore, collect as much information pertinent to the type of incident or suspected incident as possible.

2. If the privacy/security incident is ongoing (e.g., unencrypted emails containing client personal information continue to be exchanged), to the extent possible, the PSL should take immediate steps to stop or at least temporarily halt the ongoing incident.
3. **The PSL will notify the FSSA Privacy & Security Officer** of the privacy/security incident and the results of their preliminary investigation within one (1) business day from the point in time in which the PSL became aware of the privacy/security incident and began their preliminary investigation.
 - 3.1. The initial notice to the FSSA Privacy & Security Officer may be in person, by phone, or by email.
 - 3.2. The FSSA Privacy & Security Officer may direct the PSL to undertake certain actions regarding the incident, including, but not limited to, additional data collection, incident mitigation activities, preparation of a draft Incident Report, and other actions deemed reasonable at the time by the FSSA Privacy & Security Officer.

Alert: Any privacy/security incident that appears to place any of the victims of the incident or the agency at **imminent risk of harm**, the PSL should **immediately** notify the FSSA Privacy & Security Officer.

4. If an individual's **Social Security Number** has or is suspected of having been improperly disclosed, the FSSA Privacy & Security Officer will provide preliminary notification to the Office of the Indiana Attorney General.
 - 4.1. The preliminary notification must be provided within two (2) business days of when the improper disclosure occurred or is suspected of having occurred.
 - 4.2. The preliminary notification should be by email to the designated OAG contact and include as many details as are available at the time. A copy of the email should be placed in the Incident File.
5. If **FTI, SSA Data, NDNH Data, or CMS FDSH Data** has or is suspected of having been improperly disclosed or otherwise compromised, the FSSA Privacy & Security Officer will provide notification to the appropriate federal agency in accordance with the Privacy & Security Office's Incident Notification Procedures.
6. The FSSA Privacy & Security Officer, or his/her delegate, will open an **Incident File** regarding the privacy/security incident.
 - 6.1. The **Incident File** may include, but is not limited to:
 - 6.1.1. An Incident Report prepared by the FSSA Privacy & Security Officer;
 - 6.1.2. Supporting materials regarding the incident, including but not limited to:
 - 6.1.2.1. Copies of relevant emails regarding the incident
 - 6.1.2.2. Description of the CPI involved
 - 6.1.2.3. Copies of any disclosure notices prepared due to the incident
 - 6.1.2.4. Copies of relevant documents and files.
 - 6.1.3. Any other information deemed appropriate by the FSSA Privacy & Security Officer.
 - 6.2. Incident Log: The FSSA Privacy & Security Officer will maintain a log of all reported privacy/security incidents. The purpose of the log is to provide an easily referenced document of all open and closed privacy/security incidents, including status, notice provision, and reporting to HHS/OCR and/or the OAG as appropriate.
 - 6.3. Minor Incidents: Certain privacy/security incidents may be deemed minor by the FSSA Privacy & Security Officer:
 - 6.3.1. Minor incidents may be suspected privacy/security incidents that, upon investigation, are a false-positive and no real incident occurred or a similar circumstance that didn't result in any form of an unauthorized exposure of client personal information

- 6.3.2. Unless a specific request is made by a compliance agency, it's not necessary to report minor incidents to any federal and/or state agencies. Such incidents are logged in a format deemed appropriate by the FSSA Privacy & Security Officer.

Advisory: Periodically, guidance is sought from the FSSA Privacy & Security Officer by a PSL or other staff member regarding whether a certain action or activity is a privacy/security incident; in those cases where it is clearly not a privacy/security incident no documentation is required.

7. The **FSSA Privacy & Security Officer will promptly investigate the incident** to confirm and document the scope of the privacy/security incident and the associated risk to FSSA and the clients affected.
- 7.1. The FSSA Privacy & Security Officer will collect, or direct to be collected, any additional and supplemental information deemed necessary to determine the scope of the incident and to identify next step actions. FSSA personnel will fully cooperate with the FSSA Privacy & Security Officer, or his/her staff, in the investigation.
- 7.2. The FSSA Privacy & Security Officer will document the results of the investigation in the Incident Report; any supporting evidence will be captured in the Incident File.
8. The FSSA Privacy & Security Officer will establish additional Privacy & Security Office procedures, to the extent appropriate and necessary, for privacy/security incident investigation and Incident File documentation procedures, including forms and templates.

Section 5.4: Privacy/Security Incident Determination

Purpose

The purpose of this policy and its supporting procedures is to define the steps to be taken to determine the scope of any reported privacy/security incident and to identify the next action steps.

Policy

The FSSA Privacy & Security Officer will, based on the results of the investigation of any reported privacy/security incident, determine the scope of the incident and the risk, if any, to the clients involved and to the agency. The FSSA Privacy & Security Officer will collaborate with appropriate FSSA management, the FSSA Office of General Counsel (including Internal Investigations), the Office of the Indiana Attorney General, IOT and others to the extent prudent and necessary in making this determination.

The FSSA Privacy & Security Officer will complete a risk assessment utilizing any relevant federal and state risk factors, as well as any risk factors specific to the client population potentially impacted, to determine the probability that client personal information has been compromised by the incident under review.

Based on the FSSA Privacy & Security Officer's determination of scope and the results of the risk assessment, the FSSA Privacy & Security Officer will identify the next steps necessary to mitigate the risk, determine whether a breach of confidentiality has occurred, provide appropriate notice, and recommend corrective actions.

Note: based on the results of the investigation the FSSA Privacy & Security Officer will determine whether the privacy/security incident constitutes a reportable security incident to the appropriate federal agencies (e.g., IRS, SSA, OCR, CMS, OCSE, etc.) in accordance the Privacy & Security Office Incident Notification Procedures.

If client personal information has been improperly disclosed⁵ resulting in a breach (i.e., in violation of these Privacy & Security Compliance Polices, business unit policies, state security policies, and/or applicable federal and state laws and regulations), it is FSSA's policy that written notice will be provided to the victims of the improper disclosure except in cases where the risk assessment demonstrates that there is a low probability that the client personal information was compromised (and subject to the FSSA Privacy & Security Officer's discretion).

If the FSSA Privacy & Security Officer has determined that a breach has occurred, the FSSA Privacy & Security Officer will prepare or cause to be prepared appropriate written notice to the victims of the breach as provided in Section 5.5, Breach Notification, and complete the Incident Report accordingly.

If the FSSA Privacy & Security Officer has determined that a breach has not occurred, the FSSA Privacy & Security Officer will determine whether any additional training or other actions are necessary to limit

⁵ Note: The unintentional or inadvertent disclosure on client personal information that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption technology approved by FSSA is not an improper disclosure or breach unless the password or other authenticator, allowing the information to be decrypted, is known to be compromised or insufficient.

similar privacy/security incidents that did not result in a breach and recommend same to the appropriate agency, division/business unit, and/or Division of Technology Services management, as well as IOT.

Procedures

1. **Breach determination:** if a privacy/security incident that has resulted in the improper disclosure of client personal information in violation of these Privacy & Security Compliance Policies, business unit policies, state security policies, and/or applicable state and federal laws and regulations, then a breach of confidentiality has occurred subject to the exclusions identified in the above policy:
 - 1.1. If one of the above exclusions applies, the FSSA Privacy & Security Officer may still classify the incident as a breach based on the facts and circumstances of the incident (e.g., while the improper disclosure was limited, the nature of the cause of the disclosure was egregious or malicious).
 - 1.2. If none of the above exclusions apply, then the FSSA Privacy & Security Officer will provide (or cause to be provided) written notice to the victim(s) of the breach—reference Section 5.5 for breach notification procedures.
2. **Discovery Date:** The date by when notice must be provided (reference Section 5.5) for a breach is based on when the breach is first discovered by FSSA. Part of the investigation includes determining when the breach was first known to FSSA.
 - 2.1. Under the HIPAA Breach Rule, *Breaches Treated as Discovered* means that the first day on which a breach is known to FSSA or, by exercising reasonable diligence, would have been known to FSSA, is the date upon which the breach is “discovered.”
 - 2.2. This same approach to determining the Discovery Date will be used for all improper disclosures of client personal information (e.g., improper disclosure of a Social Security Number).
3. Whether or not a breach occurred, if the FSSA Privacy & Security Officer has any reason to believe the cause of the privacy/security incident was intentional or malicious or undertaken for personal gain, the FSSA Privacy & Security Officer may involve, as appropriate:
 - 3.1. FSSA Office of the Secretary (Designee)
 - 3.2. FSSA Office of Communications
 - 3.3. FSSA Human Resources
 - 3.4. FSSA Office of General Counsel
 - 3.5. Office of the Indiana Attorney General
 - 3.6. FSSA Internal Investigations
 - 3.7. Law enforcement
 - 3.8. Division/business unit management
 - 3.9. Others as deemed appropriate.

4. Whether or not a breach occurred, if the source of the privacy/security incident was or appears to be technology-based (e.g., malware attack, user authentication control compromise, ransom-ware attack, etc.), the FSSA Privacy & Security Officer will involve, as appropriate, the Division of Technology Services and the IOT Chief Information Security Officer (in accordance with the IOT Tier 1 Security Standards) in the investigation and determination of mitigating and corrective actions.
5. Whether or not a breach occurred, if the basis of the privacy/security incident is a lost or stolen portable device (e.g., laptop, USB drive):
 - 5.1. For lost or stolen laptops (including tablets and similar devices):
 - 5.1.1. Ensure that the IOT Chief Information Security Officer (or his/her designee) is informed of the situation;
 - 5.1.2. For stolen laptops, obtain a copy of the police report from the affected staff member for the Incident File;
 - 5.1.3. For state issued laptops, confirm with the IOT Chief Information Security Officer (or his/her designee) that the laptop was encrypted per the appropriate federal standard;
 - 5.1.4. Confirm with the affected staff member: (a) whether any client personal information was on the laptop; (b) that the laptop was encrypted; and, (c) that the person used a complex password (or biometric authentication) for the laptop encryption software (if applicable) and that the person's password was not lost or stolen with the device and remains secure;
 - 5.1.5. If the laptop contained client personal information and was not encrypted (or the password has been compromised), the affected staff member will need to be able to replicate the client personal information on the laptop—necessary to determine whether a breach has occurred and the number of potential victims.
 - 5.1.6. For state issued laptops, coordinate with the IOT Chief Information Security Officer (or his/her designee) regarding device remote disposition.
 - 5.2. For lost or stolen USB drives and other portable media including smart phones and tablets:
 - 5.2.1. Confirm with the affected staff member: (a) whether the media was encrypted; (b) whether the media contained client personal information; (c) if the media was encrypted that a complex password (or biometric authentication) was in use and the password was not lost or stolen with the device; (d) if the media was a smart phone or tablet that the device was enrolled in the IOT mobile device manager environment⁶; and, (e) if the media contained client personal information and was not encrypted or the password compromised, how the client personal information contained on the media can be replicated—necessary to determine whether a breach has occurred and the number of potential victims.
 - 5.2.2. For smart phones and tablets, coordinate with the IOT Information Security Officer (or his/her designee) regarding remote wiping and disabling of the device.

⁶ In accordance with IOT's Semi-managed BYOD Program and Policies and the IOT Mobile Device Policy.

5.2.3. For personally-owned smart phones and tablets that had not been enrolled in the IOT mobile device manager environment, coordinate with the staff member/owner regarding remote wiping and disabling of the device (e.g., through the person's telecommunications carrier, personal remote access accounts like MobileMe, etc.). Note that failure to enroll the device in the IOT mobile device manager environment would be a violation of IOT policy and may subject the user to potential disciplinary action, including termination of program eligibility.

6. The FSSA Privacy & Security Officer will update the Incident Report with his/her findings and conclusions.
7. The FSSA Privacy & Security Officer will apprise the associated PSL (and/or the appropriate business unit management staff) of the findings, conclusions, and next steps.

Reference [Section 7](#) regarding Laptop and Portable Device security requirements.

Section 5.5: Breach & Incident Notification

Purpose

The purpose of this policy and its supporting procedures is to define the steps to be taken to provide appropriate notice to the clients who are victims of a confirmed breach; and, to provide appropriate notice, including supplementary notice, as required under state and federal rules to the OAG, and HHS, CMS, SSA, OCSE, and IRS.

Policy

The FSSA Privacy & Security Officer is responsible for completing the notification procedures defined here in the event of a reportable security incident and/or confirmed breach of a client's personal information in FSSA's safekeeping.

In the event that the breach is caused by a Business Associate of FSSA, the FSSA Privacy & Security Officer may direct the Business Associate to prepare and provide the notices in the Business Associate's name and to absorb all costs regarding the provision of notice and any actions necessary to mitigate the deleterious effects of the breach (e.g., to pay for credit monitoring services, implement security enhancements, etc.).

Alert: The HIPAA Breach Rule requires that notice to the victim(s) of a breach must occur without unreasonable delay, but no later than 60 days after the breach was discovered (Discovery Date). IC 4-1-11 regarding the Breach of the Security of the System, in which client personal information is improperly disclosed, requires notice to be made without unreasonable delay. FSSA has been directed by the OAG to employ a thirty (30) day time limit for any notices to be provided under IC 4-1-11. IC 4-1-10 regarding the release of a Social Security Number requires notice as set forth in IC 4-1-11; however, under IAC 5-1-1 the OAG must be notified of the breach within two (2) business days of the improper release (Discovery Date) of a SSN or other personal identifying information.

Procedures

1. The FSSA Privacy & Security Officer will review the facts and circumstances of the breach regarding whether notice should be provided to the victim(s) of the breach and/or to others.
2. **OAG/Law Enforcement Coordination:** if the FSSA Privacy & Security Officer has any reason to believe the cause of the breach was intentional or malicious or undertaken for personal gain, the FSSA Privacy & Security Officer will involve the OAG and/or law enforcement personnel (including OGC Internal Investigations), as appropriate:
 - 2.1. The OAG or law enforcement may determine that a delay in providing notice to the victim is necessary to avoid any compromise of the investigation. If a delay is necessary:
 - 2.1.1. The OAG/law enforcement must provide the FSSA Privacy & Security Officer with a written directive requesting the delay (including the reason for the delay) and the time period of the delay.

2.1.2. The FSSA Privacy & Security Officer will document the directive in the Incident Report and delay the provision of notice for the time period specified in the directive.

2.1.3. The FSSA Privacy & Security Officer can delay the provision of notice based on a verbal request from the OAG/law enforcement (documenting same in the Incident Report), but the delay cannot exceed thirty (30) calendar days from the date of the verbal request.

3. **Improper disclosure of a Social Security Number:** If a client's Social Security Number is disclosed in violation of IC 4-1-10, the FSSA Privacy & Security Officer will provide notice of the incident to the OAG within two (2) business days from the Discovery Date in accordance with 10 IAC 5-1-1.

3.1. This notice to the OAG may be preliminary pending confirmation that an actual disclosure of a SSN occurred (i.e., an improper disclosure of a SSN is suspected, but unconfirmed; providing preliminary notice within the two (2) business day timeframe satisfies 10 IAC 5-1-1, even if the OAG notice is retracted later should it be determined that a SSN was not improperly disclosed).

3.2. This notice may be by email and should indicate that an investigation is underway, and steps have been taken, as appropriate, to stop any continuation of the improper disclosure.

3.3. If it is confirmed that an SSN was improperly disclosed, once the investigation is complete and notice provided to the victim, a copy of the notice and the Incident Report is to be sent to the OAG for their files.

Note: it has been past practice for the OAG to subsequently send a letter to the FSSA Privacy & Security Officer indicating whether or not FSSA fulfilled the requirements of the law regarding SSN improper disclosures; the letter should be filed in the Incident File.

4. **Notice to Individuals:**

4.1. Timing of Notice: Written notice to the victim(s) of a breach will be provided without unreasonable delay and in no case not later than thirty (30) calendar days after the Discovery Date if a social security number was disclosed (unless otherwise delayed by the OAG/law enforcement). If a social security number was not disclosed, written notice will be sent without unreasonable delay, but in no case not later than sixty (60) days from the Discovery Date.

4.2. Content of Notice and Distribution:

4.2.1. The written notice to the victims will be written in plain language and include the elements required under the HIPAA Breach Rule (including notices for breaches that do not involve PHI or are otherwise not a violation of the HIPAA Privacy Rule):

4.2.1.1. A Disclosure Notice template—prepared and maintained by the Privacy FSSA Officer—provides the appropriate format and content requirements, with options based on the type of information disclosed (e.g., credit bureau contact information in the event of a financial or SSN disclosure).

4.2.2. The written notice will be sent to the victim(s) by first class mail, USPS, at their last known address; in certain cases, as determined by the FSSA Privacy & Security Officer based on the facts and circumstances of the situation, written notice will be provided to the victim's authorized

representative/personal representative/parent/legal guardian in addition to or in lieu of the victim.

4.2.3. At this juncture, delivery of written notice by email is not approved.

4.2.4. IC 4-1-11-9 Alternate Form of Notification: If the breach is clearly not the result of a violation of the HIPAA Privacy Rule and the conditions of IC 4-1-11-9 are met, the FSSA Privacy & Security Officer, in collaboration with the FSSA Office of General Counsel and the FSSA Director of Communications, may use the alternative form of notification as provided for in IC 4-1-11-9.

4.3. Urgent Situations: In situations that the FSSA Privacy & Security Officer deems urgent due to the nature of the breach (e.g., possible imminent misuse of client personal information resulting in identity theft), FSSA may provide information to the victims by phone or other means as determined by the FSSA Privacy & Security Officer. Provision of written notice is still required.

4.4. Notice to Media: If the breach is a violation of the HIPAA Privacy Rule (as determined by the FSSA Privacy & Security Officer) and involves more than 500 victims (individuals), notice to the media is required in accordance with the HIPAA Breach Rule:

4.4.1. Providing notice to the media will be done in accordance with the HIPAA Breach Rule with respect to timing (same time period as providing notice to the individual victims), content, and distribution (e.g., to prominent media).

4.4.2. The FSSA Privacy & Security Officer will collaborate with the FSSA Communications Director in drafting the media notice and its distribution.

4.4.3. Website Posting:

4.4.3.1. In addition to media notice, notice will be conspicuously posted on FSSA's website home page regarding the breach and include appropriate contact information.

4.4.3.2. A toll-free number and email address will be provided for individuals to contact FSSA about the breach.

4.4.3.3. The posting will remain on the website for no less than ninety (90) calendar days.

4.4.3.4. To the extent deemed appropriate by the FSSA Communications Director, a summary notice also may be posted on the state's website home page with a link to the FSSA webpage.

Inquiry Response: The FSSA Privacy & Security Officer will collaborate with the FSSA Communications Director regarding FSSA's response content and procedures for responding to individual and media inquiries.

Alert: FSSA has the burden of proof under federal regulations to demonstrate that either a breach, in fact, did not occur; or, that all appropriate actions and notices were undertaken in a timely manner. All of the actions taken, including copies of notices, should be documented in the Incident Report and Incident File as a means to provide this proof.

5. Notice to Federal and State Agencies:

- 5.1. The FSSA Privacy & Security Officer will determine whether notice of the privacy/security incident is reportable to one or more federal or state agencies in accordance with Sections 5.7 and 5.8 and the FSSA Privacy & Security Office Incident Notification Procedures.
- 5.2. Certain privacy and security incidents that did not result in a breach may still be reportable to the applicable federal agencies. The FSSA Privacy & Security Officer will make this determination in accordance with the FSSA Privacy & Security Office Incident Notification Procedures.

Section 5.6: Mitigation & Corrective Actions

Purpose

This policy has three purposes:

1. To establish the requirement that FSSA undertake all reasonable actions to mitigate the deleterious (harmful) effects of any breach experienced by the agency.
2. To identify appropriate and reasonable corrective actions to be undertaken to minimize the risk of subsequent, similar breaches.
3. For privacy/security incidents that did not result in a breach, to identify appropriate and reasonable corrective actions to reduce associated risk that a similar privacy/security incident does not subsequently result in a breach or other improper use of client personal information.

Policy

1. The FSSA Privacy & Security Officer will direct reasonable actions to be undertaken by the affected business units and/or Business Associates to mitigate the deleterious effects of any breach, including any actions necessary to stop an ongoing breach. FSSA division management will be responsible to undertake these actions in a timely manner.
2. *Spillage:* Spillage is defined as client personal information (or other sensitive information) that is inadvertently placed on, subsequently shared with, or distributed to personnel or information systems that are not authorized to process such information. The inadvertent disclosure of CPI to a third party not authorized to receive the CPI and the inadvertent downloading of CPI to an unauthorized device (such as a smart phone or tablet) would be two examples of spillage. In the event of spillage, the FSSA Privacy & Security Officer, in collaboration with others as appropriate, will identify the information involved, assure the FSSA and IOT incident response personnel are alerted (employing a communication method not associated with the spill), identify the systems/personnel/components that received the information, and take appropriate steps to obtain (have the spilled information returned), remove, or destroy the spilled information. These actions are integrated with the incident determination and containment procedures outlined in procedures below and this Section 5, including the determination of whether the spillage resulted in an improper disclosure.

3. If a Business Associate is involved with the breach—whether the source of the breach, a contributor, or in a position to effectively assist with mitigation activities—the responsible business unit will work with and, to the extent appropriate, oversee the mitigation activities of the Business Associate.
4. FSSA division management is responsible to assess and implement corrective actions reasonably identified by the FSSA Privacy & Security Officer and/or division personnel to minimize the risk of subsequent, similar breaches.
 - 4.1. Division management's assessment may include the identification of alternative, but equally effective corrective actions (in lieu of the corrective actions identified by the FSSA Privacy & Security Officer).
 - 4.2. The assessment is to be completed within a reasonable period of time, based on the scope and complexity of the identified corrective action; division management will provide the FSSA Privacy & Security Officer a timeline in which the assessment and their determination will be completed.
 - 4.3. If, based on their assessment, division management determines that the cost or complexity of the corrective action is greater than the associated risk—that is, division management is willing to assume the risk of a subsequent, similar breach and not invest in the corrective action—they must document that determination and risk acceptance in a formal memo to the FSSA Privacy & Security Officer for inclusion in the Incident File.
5. For privacy/security incidents that did not result in a breach, the FSSA Privacy & Security Officer may identify corrective actions to prevent similar privacy/security incidents from occurring (that may result in a breach or other improper use of client personal information).
 - 5.1. This may include other issues and risks identified during the course of a privacy/security incident investigation that need to be addressed to avoid a subsequent privacy/security incident.
 - 5.2. FSSA division management is responsible to assess and implement these corrective actions.
 - 5.3. The assessment is to be completed within a reasonable period of time, based on the scope and complexity of the identified corrective action; division management will provide the FSSA Privacy & Security Officer a timeline in which the assessment and their determination will be completed.
 - 5.4. If, based on their assessment, division management determines that the cost or complexity of the corrective action is greater than the associated risk—that is, division management is willing to assume the risk of a subsequent, similar privacy/security incident and not invest in the corrective action—they must document that determination and risk acceptance in a formal memo to the FSSA Privacy & Security Officer for inclusion in the Incident File.

Advisory: Corrective actions are dependent on the situation and the facts and circumstances of the incident and may range from staff member counseling to developing system modifications to significantly changing business processes. For large-scale and/or complex corrective actions, the FSSA Privacy & Security Officer will collaborate with division management with identifying reasonable corrective actions.

Simple corrective actions (e.g., counseling or retraining a staff member) may be completed and documented for inclusion in the Incident Report by business unit management without a formal assessment as described above.

Procedures

Appropriate mitigation and corrective action procedures are dependent on the situation and the facts and circumstances of the breach or privacy/security incident, and will need to be determined on a case-by-case basis. The following are intended to provide guidance, unless otherwise stated. The FSSA Privacy & Security Officer will document the mitigation and recommended corrective action procedures in the Incident Report.

1. **Stop On-going Breach:** If a breach of client personal information is ongoing—for example, provider manual containing client personal information in example screen shots is posted on a public website—the first action item is to take all reasonable actions to stop the breach; in this example, remove the manual from the website or shut down the website.
 2. **Return Request:** Client personal information improperly disclosed by tangible means should be retrieved from the recipient as soon as possible:
 - 2.1. Tangible means is a physical document (e.g., notice, letter, appeal hearing packet), an electronic file (e.g., spreadsheet, email), a device (e.g., USB drive), or similar.
 - 2.2. Upon learning that client personal information was improperly disclosed by tangible means, staff personnel should immediately contact the recipient and ask for its return—record the date contact was made and the name and contact information of the recipient.
 - 2.2.1. If necessary, a self-addressed stamped envelope may be sent to the recipient to return physical documents or devices. The FSSA Privacy & Security Officer can assist; see 2.3 below.
 - 2.2.2. If the tangible means was an electronic file sent by email or other electronic means, ask the recipient to completely delete the file (from their inbox, deleted items, folders, and recycle bin), and to send you a confirmation email that they did so.
 - 2.2.3. If the tangible means was client personal information contained in an email, ask the recipient to completely delete the email (inbox, deleted items, any other mail folder or folder), and to send you a confirmation email that they did so.
- Advisory:*** Do not ask the recipient to “destroy” physical documents or devices. FSSA wants it returned so that we can be assured of its proper destruction. For some, “destroy” may simply mean “toss it in the trash.”
- 2.3. **Disclosure Return Request/Attest Letter:** in most cases in which client personal information was improperly disclosed to an individual, the FSSA Privacy & Security Officer will send or cause to be sent a letter to the recipient that:
 - 2.3.1. Asks for the return of the client personal information, if it has not already been returned.

2.3.2. Asks the recipient to attest in writing (by signing and returning the letter) that they did not retain, use, or further disclose the client personal information improperly sent to them.

2.3.3. A stamped, self-addressed (to the FSSA Privacy & Security Officer) envelope will be included.

Alert: If OCR investigates a breach, it will ask what efforts were made to retrieve client personal information that was improperly disclosed, if it was in tangible form (as described above).

3. **Corrective Actions:** Within sixty (60) calendar days of a reported privacy/security incident, whether or not the incident resulted in a breach, the FSSA Privacy & Security Officer, in collaboration with the business unit originating the privacy/security incident and others as deemed appropriate by the FSSA Privacy & Security Officer, identify recommended corrective actions to minimize the risk of a reoccurrence of a similar or associated privacy/security incident. The corrective actions may include, but are not limited to:

3.1. **Counseling/Retraining:** In cases where a lack of privacy discipline on the part of a FSSA staff member is the source of a privacy/security incident/breach, the FSSA Privacy & Security Officer may recommend that the staff member be counseled by their supervisor on the matter and, perhaps, be retrained on FSSA's Privacy & Security Compliance Policies and the business unit's privacy policies and procedures.

3.1.1. Such counseling and/or retraining should be documented in the staff person's file with a confirming email to the FSSA Privacy & Security Officer (for the Incident File) as evidence that the counseling and/or retraining occurred (including date).

3.1.2. In certain cases, the FSSA Privacy & Security Officer may recommend that all staff personnel involved in similar services subject to the privacy/security incident be formally "reminded" of the appropriate confidentiality policies and procedures. The formal reminder may be in whatever form best suits the business unit; a confirming email should be sent to the FSSA Privacy & Security Officer for inclusion in the Incident File as evidence that the formal reminder occurred (including date).

3.2. **System/Process Modifications:** In cases where the FSSA Privacy & Security Officer has recommended changes to application systems and/or business processes to minimize the risk of similar or associated privacy/security incidents (whether or not a breach has occurred):

3.2.1. The affected division and business unit should assess the cost, complexity, and likelihood the modification will achieve the risk reduction objective, and made a determination as whether to accept the risk, implement an alternative but equally effective modification, or to proceed with the recommended modification.

3.2.2. The affected division and business unit should apprise the FSSA Privacy & Security Officer of their determination.

- 3.2.2.1. If the determination is to accept the risk (and make no changes), the division must communicate this decision in a formal memo to the FSSA Privacy & Security Officer for the Incident File.
- 3.2.2.2. If the determination is to make the modification, the division and business unit should report their progress on a periodic and timely basis to the FSSA Privacy & Security Officer until completion (so that progress and completion may be documented in the Incident File).
- 3.3. Policy & Procedure Changes: The basis for the privacy/security incident may be a result of missing or insufficient policies and/or procedures at the agency and/or business unit level. The FSSA Privacy & Security Officer may recommend appropriate changes on such policies and procedures for enactment by the agency and/or the business unit.
- 3.4. Personnel Actions: Any resulting personnel actions are the responsibility of the business unit. The FSSA Privacy & Security Officer may recommend the business unit consider disciplinary action for staff who repeatedly violate these Privacy & Security Compliance Policies and/or the business unit's policies and procedures.

Section 5.7: Notice to HHS

Purpose

Under federal regulations, FSSA is required to report to HHS/OCR breaches that involved the disclosure of PHI. The purpose of this policy is to ensure the timely reporting of such breaches.

Note: improper disclosures of Social Security Numbers are also to be reported to the Office of the Indiana Attorney General; [Section 5.5](#) addresses this requirement.

Policy

The FSSA Privacy & Security Officer is responsible for notifying HHS/OCR of breaches involving PHI in accordance with the HIPAA Breach Rule, and for maintaining a log of all such breaches.

For breaches that are caused by a Business Associate, either the FSSA Privacy & Security Officer or the Business Associate will provide notice to HHS/OCR depending on the circumstances and as directed by the FSSA Privacy & Security Officer.

Procedures

1. ***Incident Tracking Log:*** The FSSA Privacy & Security Officer will maintain a master log of all privacy/security incidents, which also identifies those incidents resulting in a breach that is reportable to HHS/OCR. The form and format of the log is at the discretion of the FSSA Privacy & Security Officer.
 - 1.1. The objective is to maintain a comprehensive list of all suspected and confirmed privacy/security incidents.
 - 1.2. Incidents resulting in a breach of PHI will be so identified, and the date each such incident is reported to HHS/OCR will be documented on the log.
 - 1.3. The FSSA Privacy & Security Officer will update the incident tracking log contemporaneously with any actions taken with respect to each privacy/security incident.
2. ***Notice to HHS/OCR:***
 - 2.1. If the breach results in notice to the victims of the breach and PHI was improperly disclosed, the FSSA Privacy & Security Officer (or Business Associate) will provide notice to HHS/OCR:
 - 2.1.1. If 500 or more individuals (victims) are subject to the breach, the FSSA Privacy & Security Officer (or Business Associate) will provide notice to HHS/OCR contemporaneously with providing notice to the victims.
 - 2.1.2. If fewer than 500 individuals (victims) are subject to the breach, the FSSA Privacy & Security Officer (or Business Associate) will provide notice to HHS/OCR:
 - 2.1.2.1. Either contemporaneously with providing notice to the victims; or,
 - 2.1.2.2. Not later than sixty (60) calendar days after the end of the calendar year in which the breach occurred.
 - 2.1.3. Notice to HHS/OCR is made via its website (subject to change by HHS/OCR):

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

- 2.2. If the breach results in notice to the victims of the breach and PHI was improperly disclosed, and the source of the breach is a Business Associate:
 - 2.2.1. If the Business Associate is also a Covered Entity under the HIPAA rules, the Business Associate typically would provide notice to HHS/OCR:
 - 2.2.1.1. The FSSA Privacy & Security Officer will determine, based on the circumstances, whether collaboration with the Business Associate is necessary regarding the content and timing of the notice to HHS/OCR.
 - 2.2.1.2. The FSSA Privacy & Security Officer will determine, based on the circumstances, whether a copy of the notice to HHS/OCR is needed for the Incident File.
 - 2.2.1.3. These determinations will be documented in the Incident Report and noted on the incident tracking log by the FSSA Privacy & Security Officer.

Section 5.8: Notice to Other Federal Agencies

Purpose

Under federal regulations, FSSA may be required to report privacy/security incidents to certain federal agencies depending on the nature of the privacy/security incident. The purpose of this policy is to ensure the timely reporting of such incidents.

Policy

The FSSA Privacy & Security Officer has developed Privacy & Security Office Incident Notification Procedures, incorporated herein by reference, that address the timely reporting of certain privacy/security incidents to the appropriate federal and state agencies, including but not limited to Centers for Medicare and Medicaid Services (CMS), the Social Security Administration (SSA), the HHS/Office of Child Support Enforcement, and the Internal Revenue Service (IRS), as well as the method and means of such reporting.

Guidance: Under federal rule, potential or confirmed security incidents (including a breach) that affect PII provided to the agency by CMS through the Federal Data Services Hub (FDSH) are to be reported to CMS within one (1) hour of discovery following the procedures outlined in the *CMS Administering Entity Security and Privacy Incident Response and Guidance* document (currently, Version 1.0, December 16, 2016).

With respect to Federal Tax Information received by agency from the IRS and the SSA, in accordance with Section 10 of IRS Publication 1075 potential or confirmed security incidents (including a breach) that include or may include the improper inspection or disclosure of such FTI must be reported to the IRS immediately, but no later than within twenty-four (24) hours.

With respect to PII that includes SSA-provided information received by the agency from the SSA, in accordance with the *SSA Electronic Information Exchange Security Requirements and Procedures* document and the Information Exchange Agreement (executed between the agency and the SSA), potential or confirmed security incidents (including a breach) must be reported to the SSA within one (1) hour of discovery.

With respect to the National Directory of New Hires (NDNH) information received from the HHS Office of Child Support Enforcement (OCSE), in accordance with the Computer Matching Agreement with OCSE, potential or confirmed breaches of NDNH information must be reported to OCSE within one (1) hour of discovery.

The Privacy & Security Office Incident Notification Procedures delineate the types of reportable incidents and establishes thresholds for incident reporting, including the adoption of the methods and means of reporting to the appropriate federal agencies as outlined in the documents referenced above and as further established in the Procedures. As may be required from time-to-time, additional notification requirements (e.g., with other federal or state agencies), may be added to the Incident Notification Procedures by the FSSA Privacy & Security Officer.

Section 6: Email Policy

Purpose

The purpose of this policy is to establish the rules and procedures to be followed by FSSA and its personnel (workforce members) with respect to use of electronic mail (email).

Background

Email is a primary business communication tool employed by FSSA (and most organizations). It provides a convenient and traceable means to exchange information among staff members, clients, service providers, and the public. However, email can be a significant source of privacy/security incidents, if not used judiciously.

In the normal conduct of business, email is used to send and receive client personal information, as well as other agency sensitive information. This is both a necessary and appropriate use of email technology, and, generally stated, is more secure and cost effective than other information exchange technologies like faxing, provided appropriate controls are used to protect the information from improper disclosure or compromise.

It is important to note that the improper use of email, whether intentional or unintentional, is a major source of privacy/security incidents, including those that result in a breach of confidentiality. Two common causes of such incidents are misdirected email—i.e., sent to the wrong person; and, emailing client personal information insecurely Outside the State Network—i.e., unencrypted email sent to a **non-fssa.in.gov** address.

Therefore, specific email policies and procedures are necessary to direct and guide FSSA personnel in the appropriate use and protection of email; not to hinder communications, but rather to minimize the risk of client personal information being improperly used or disclosed.

Policy

All FSSA personnel are required to comply with this email policy, as further defined in the following sub-sections.

Section 6.1: Email Rules

Purpose

The purpose of this policy is to establish the rules regarding email use by FSSA personnel.

Policy

All FSSA personnel will follow these rules regarding their use of email in the conduct of state business on behalf of FSSA.

1. Email content and attachments are subject to the Use and Disclosure Policy defined in these Privacy & Security Compliance Policies ([Section 1](#)). Only personnel so authorized by their business unit may send client personal information by email.

Advisory: Before sending client personal information by State Email, ask yourself:

- (1) Is it necessary to include the information?
- (2) Is there a better means to communicate the information other than by email (e.g., phone call or hand delivery, *but not fax*); and,
- (3) Do I need to encrypt the information (see [Section 6.2 Email Security](#))?

Always minimize the amount of client personal information in any email to the least possible amount needed—**Minimum Necessary Applies to State Email, as well.**

2. State Email that **contains client personal information**, including any attachments, **cannot be sent Outside the State Network** unless the message and any attachments are secured as specified in [Section 6.2 Email Security](#).

Alert: Sending a State Email that contains client personal information, including any attachments, Outside the State Network that has not been secured in accordance with Section 6.2 Email Security is a violation of these Privacy & Security Compliance Policies, constitutes a privacy/security incident, and may result in personnel sanctions in accordance with state and FSSA policy.

3. State Email that contains **client personal information**, including any attachments, may be sent Inside the State Network without the additional security precautions as specified in [Section 6.2 Email Security](#). The sender, however, should consider the volume and types of client personal information being sent and the number of recipients, and encrypt the email message and/or attachments (as described in Section 6.2) if additional protection is appropriate under the circumstances.
4. Under no circumstances is Federal Tax Information received by the agency from the Internal Revenue Service or the Social Security Administration to be emailed. Such information must be otherwise securely communicated (contact the FSSA Privacy & Security Officer for guidance). Inadvertent

emailing of FTI must be reported as an incident in accordance with Section 5.2 of these Privacy & Security Compliance Policies.

5. Subject Line: **Never put client identifying information** in the Subject Line of an email.

5.1. Refer to [Section 6.2 Email Security](#).

6. Personnel may not store state information such as email attachments on non-State-owned equipment or devices except as provided for in [Section 7 Portable Device Policy](#).
7. Personnel will comply with the IOT Tier 1 Security Standards regarding prohibited email practices (reference IOT-CS-SEC 115 and 129).
8. Personnel may access their State Email remotely using, for example, mobile/smart phones and home computers, subject to the restrictions and guidance in [Section 7 Portable Device Policy](#).
9. Personnel may not allow another person, whether or not they are a workforce member, to use their State Email Account. This would be a violation of state security policy (IOT Tier 1 Security Standards) and the Information Resource Use Agreement (IRUA) signed by the staff member, and a violation of these Privacy & Security Compliance Policies.

Alert: Allowing someone else to use your State Email Account, including giving them your password to state systems, besides being a violation of policy, means anything they do under your name can and will be traced back to you. With your password and/or your State Email Account, everything this person does will be assumed to be you.

10. State Emails should be sent only to **known** businesses, clients, or other State Emails accounts:

10.1. **Personnel are individually responsible** to ensure State Emails are sent only to the **intended and authorized recipient**; misdirected email may result in a privacy/security incident.

Caution: Outlook automatically populates email addresses based on the first few letters of the recipient's name or email address you type in. It is very easy to accidentally send an email to John.Doe@doc.in.gov instead of the intended recipient Jan.Doe@fssa.in.gov.

11. Signature Block and Confidentiality Notice: All State Emails that contain client personal information (in the message and/or as attachments) are to include the following signature block:

Your name

Your contact information (title, phone number, email address)

[And, the following confidentiality notice approved by the Office of General Counsel:]

Confidentiality Notice: This communication, including any attachments, may contain confidential or privileged information. If you have received this communication in error, please notify the sender by reply email and destroy all copies of the message and any attachments; do not copy or further transmit the message or any attachments.

12. Personnel who become aware of a violation or possible violation of this policy are to report the violation to their supervisor; if the supervisor is not available, then it should be reported to the assigned Privacy/Security Liaison. Violations of this policy can lead to a privacy/security incident, as well as staff member sanctions in accordance with FSSA and state policy.

12.1. The supervisor (or PSL) will review the situation and take appropriate corrective action.

12.2. If it appears that the violation has resulted in a privacy/security incident, the supervisor (or PSL) will act in accordance with [Section 5 Incident Management and Breach Reporting](#) of these Privacy & Security Compliance Policies.

Procedures

None under this policy. Business Units may develop more detailed email procedures, as needed, and such procedures may be more restrictive depending on the business need.

Section 6.2: Email Security

Purpose

The purpose of this policy and its supporting procedures is to establish the rules regarding securing email content to protect the confidentiality and integrity of any client personal information that may be legitimately communicated by State Email.

Policy

It is FSSA's policy that:

1. Any State Email that contains, including attachments, client personal information that is to be sent Outside the State Network must be properly secured through the use of encryption technologies, as described in this section.
2. It is the individual staff member's responsibility to properly secure any State Email the individual sends (including Replies and Forwards) Outside the State Network that contains client personal information and ensure that it is sent to only the intended recipient.
3. It is the individual staff member's responsibility to ensure any State Email the individual sends (including Replies and Forwards) Inside the State Network that contains client personal information is sent to only the intended recipient.
4. All State Email sent Outside the State Network will be automatically scanned by IOT to detect client personal information. This will help detect and prevent the unauthorized disclosure of client personal information by email.
5. Under no circumstances may an FSSA workforce member utilize their personal email account (e.g. Gmail, Yahoo, etc.) for sending and/or receiving any FSSA client personal information.

Procedures

1. Any State Email that contains client personal information *and* is to be sent **Outside the State Network** (i.e. any address not containing an fssa.in.gov extension) shall only be sent using an approved email encryption tool. ***The FSSA Privacy & Security Office can be contacted for guidance on the proper encryption tool.***
2. Any State Email attachments that contain client personal information sent Inside the State Network can be further protected through an encryption method approved by the FSSA Privacy & Security Officer. This would add protection against inadvertently emailing client personal information to the wrong address and/or to further protect highly sensitive information.

Advisory: For highly sensitive documents or files with large amounts of client personal information that you need to send Outside the State Network, it is strongly recommended that you encrypt those documents using an encryption method approved by the FSSA Privacy & Security Office *and* use an approved email encryption tool.

You can send the password to the recipient by separate email, but you must be sure the recipient's address is correct and verify the correct recipient received your password, or ask them to reply that they received the password before sending the document. If you routinely exchange encrypted documents with a recipient, you can establish a pre-arranged password with the recipient to be used for all such documents. However, the prearranged password should be changed at least every 60 calendar days.

Global Address List Issue:

Outlook has a feature that automatically populates the To, CC, and BCC address boxes in an email message based on the first few characters you type in.

Be careful! You can easily send your email to the wrong person—always review the email addresses before you press Send or Send Secure.

All FSSA personnel have access to the Global Address List, which contains the email addresses of everyone with a State Email Account, plus a large number of non-in.gov addresses. This is to make it convenient for you to find someone's email address.

Be careful! It is easy to select the wrong person from the Global Address Book. You might mean to select John.Doe@fssa.in.gov, but inadvertently selected Jon.Doe@isdh.in.gov whose address appears right next to John's in the Global Address List.

While the email message and any attachments are secure during transit Inside the State Network, if the wrong recipient receives your email a privacy/security incident may have occurred.

To minimize the risks of sending a misdirected email message containing client personal information Inside the State Network, it is recommended that you encrypt the message and/or attachments following the procedure described above.

Section 6.3: Using a Scanner to Scan/Send Client Personal Information

Many business units have printer/copier/scanners (multifunction devices, or MFD's) that can be used to scan and email documents. Most of these scanners have the ability to encrypt the scanned document.

The same security rules apply to documents scanned and emailed from a scanner as apply to email, reference [Section 6.2](#) above.

If the scanned document contains client personal information and it is to be emailed Outside the State Network, the document must be encrypted.

If the scanned document contains client personal information and it is to be emailed Inside the State Network, the document should be encrypted to minimize any risk should the document be inadvertently emailed to the wrong address.

If the MDF does not have the capability to encrypt the document to be scanned, an option is to scan and email the document to yourself and then encrypt and email the document as described in Section 6.2 above.

Section 7: Laptop & Portable Device Policy

Purpose

The purpose of this policy and its supporting procedures is to establish the rules regarding portable devices employed by FSSA personnel, including laptops and smart phones, as well as the use of personally-owned computers to access State Email.

Background

Many FSSA staff are assigned a laptop computer for daily use instead of a desktop computer. Other FSSA staff may periodically use a laptop from their business unit's loaner pool when portable computing is needed. Laptops present a particular security risk given that they are subject to theft and loss.

Some FSSA staff members have the use of a state issued smart phone capable of receiving and sending email; some staff use personal smart phones for this purpose. The use of smart phones to send and receive State Email is generally permitted as long as certain rules are followed to ensure the protection of client personal information.

Likewise, many FSSA staff members access their State Email Accounts from their personally owned computers over the Internet using State Webmail (IOT provided Internet access to outlook.office365.com, which includes your State Email, calendar, and contacts). Doing so is generally permitted provided the staff member follows the requirements of both FSSA Privacy and Security and the Indiana Office of Technology. Accessing any IOT-provided cloud resources (State Webmail, SharePoint Online, CRM Online, etc.) outside of the State of Indiana network on personally owned laptops, desktops or smart phones will require users to be enrolled with multi-factor authentication through IOT.

Portable media devices, including USB drives, external hard drives, CD/DVD's, and tape present some unique security issues given the ease by which such devices can be lost or stolen. This policy significantly limits what types of portable media may be used to hold client personal information and requires that all such devices be encrypted.

Policy

1. FSSA personnel may use either state-owned or approved personally owned smart phones or similar devices (e.g., tablets, notepads) to access State Email containing client personal information provided appropriate security controls are in place as described in the Procedures section of this policy.
2. FSSA personnel may use personally-owned personal computers (desktops, laptops, etc.), smart phones, and similar devices to access State Email containing client personal information via State Webmail (<https://outlook.office365.com>) provided appropriate security controls are in place as described in the Procedures section of this policy.
3. With respect to portable media: FSSA personnel may not transfer client personal information to any portable media except FSSA approved and encrypted USB drives and external hard drives.
 - 3.1. The use of any other portable media such as CD's, DVD's, tape, unapproved USB drives, and unapproved external hard drives **is strictly prohibited**.

- 3.2. Client personal information should not be transferred to any portable media unless absolutely necessary for business purposes.

3.2.1. FSSA staff are responsible for the security of client personal information copied to portable media including the ability to completely replicate all of the client personal information should the portable media be lost or stolen.

4. With respect to laptops: FSSA personnel may not transfer client personal information to any laptop that is not encrypted in accordance with FSSA's encryption standard.

- 4.1. Client personal information may be transferred only to state-owned laptops unless prior permission is granted by the appropriate business unit management for a staff member to use a non-state-owned laptop:

- 4.1.1. Contractors (that meet the definition of workforce member) are often required to provide their own laptops; that is, they are not issued a state-owned laptop. Such contractors may transfer client personal information to their laptops provided that:

- 4.1.1.1. Doing so is a necessary course of business for the contractor in order for them to fulfill their contractual obligations to FSSA;

- 4.1.1.2. The contractor's host business unit management (who has engaged the contractor) has authorized placing client personal information on the laptop;

- 4.1.1.3. The laptop is encrypted in accordance with FSSA's encryption standards and protected with a complex password (or biometric authenticator);

- 4.1.1.4. The laptop has up-to-date anti-virus and firewall technology in place; the anti-virus and firewall technology must meet or exceed the functionality of the state's anti-virus and firewall technology employed on state-owned laptops; and, the anti-virus and firewall technology must be kept up-to-date at all times (e.g., through a subscription service with the vendor of the technology).

- 4.1.1.5. The contractor fully agrees to be responsible for the security and confidentiality of any client personal information on the laptop, including providing appropriate and secure backup or the ability to otherwise completely replicate the client personal information; and,

- 4.1.1.6. The contractor will fully and completely remove all client personal information from the laptop: (1) when it is no longer necessary for the contractor's work for FSSA or (2) upon completion of the contractor's engagement to FSSA, including if the contractor is reassigned to a different FSSA business unit and the client personal information is not applicable to the contractor's new assignment.

- 4.1.2. FSSA staff should avoid copying client personal information to a laptop unless absolutely necessary for business purposes:
 - 4.1.2.1. FSSA staff are responsible for the security of client personal information copied to a laptop including the ability to completely replicate all of the client personal information should the laptop be lost or stolen.**
 - 4.1.2.2. Once the client personal information is no longer needed on the laptop, the staff person who copied the information to the laptop is responsible to completely remove all of the client personal information from the laptop (including recycle bin).
 - 4.1.3. State-owned laptops may not be taken offsite (out of the state government offices) unless authorized by the staff person's business unit management. This authorization may be included in the individual's job description; it may be conferred by email; or, it could be defined in the business unit's policies and procedures (e.g., staff at a certain level are permitted to take their assigned laptop offsite).
5. Password Protection: These Privacy & Security Compliance Policies and the IOT Tier 1 Security Standards (reference IOT-CS-SEC-117) require the use of complex passwords for all user accounts; this includes passwords for laptops, portable media, and encrypted documents. For smart phones and tablets a complex passcode of at least six (6) digits and/or a biometric authenticator (e.g., fingerprint recognition) may be employed in lieu of a complex password provided the device is enrolled in the IOT mobile device management platform MobileIron.
 - 5.1. **Sharing of your password or passcode with someone else is a direct violation of this policy.**
 - 5.2. Placing a copy of your password/passcode on or with a laptop or portable media device or smart phone is the same as sharing your password/passcode. If the device is lost or stolen, the contents will not be protected, whether or not it is encrypted, if your password/passcode is compromised.
6. Any client personal information that must be transferred for use by FSSA staff, including contractors (workforce members)—for example, creating or using an Excel spreadsheet or Word document—shall only be retained in a secure location approved by the FSSA Privacy & Security Office, and not on a laptop or similar device.
7. Client personal information **shall not be copied to any web storage locations** (e.g. Google Drive, Apple iCloud, Dropbox, Carbonite, etc.) that have not been approved by the FSSA Privacy & Security Office. FSSA workforce members are responsible for verifying "auto backup" features are turned off of all devices (i.e. smartphones, iPads, laptops, desktops, etc.) to avoid an inadvertent transfer of client personal information to an unauthorized web storage location.
8. In the situation that workforce members will be traveling to locations the agency deems to be of significant risk, as needed the agency will issue specially configured mobile devices (smartphones, laptops, etc.) designed to minimize the risk of unauthorized exposure to client personal information and/or other sensitive information. It is incumbent on the FSSA business unit to coordinate with agency leadership, including the FSSA Privacy & Security Officer, and the Indiana Office of Technology

(IOT) regarding any such travel plans to confirm that the appropriate risk mitigation measures are in place prior to the individual travelling.

9. Each FSSA staff person is responsible to comply with this policy and is responsible to help maintain adequate security over their use of portable devices and laptops.
10. Only approved software may be installed on state owned devices (e.g. laptops, desktops, portable devices, smartphones, etc.). This approval should be received from the FSSA Privacy & Security Office. Once software has been approved by the FSSA Privacy & Security Office, it's the responsibility of the FSSA workforce member to promptly install updates and/or patches as necessary to minimize any security risks involved with the use of the software.

Procedures

A. Using smart phones, tablets, and similar devices:

1. This procedure applies to state issued devices and approved personally owned (or contractor owned) devices used for state business purposes in which client personal information is accessed, including State Email.
2. The **password or passcode is to be changed** at least every sixty (60) days or sooner if required by federal and/or state law. The password or passcode is not to be stored with or on the device.
3. The device is to be encrypted in accordance with FSSA's encryption standards. This is to include any removable memory cards used by the device. The device is to have up-to-date anti-virus and firewall technology in place that meets or exceeds the IOT requirements under the IOT Mobile Device Policy.
4. Any device utilized to access CPI shall be promptly updated to the latest version of the appropriate operating system (e.g. current iOS). Failure to promptly update the operating system may result in a loss of your ability to utilize the device to access CPI.
5. SMS text messages are inherently insecure. Thus, sending any sensitive CPI via an SMS text message is strictly prohibited. FSSA workforce members should consult with the FSSA Privacy & Security Office for a secure alternative to sending SMS text messages.
6. Under no circumstances shall FTI be accessed via a mobile device such as a smart phone and/or tablet (e.g. iPad).
7. In accordance with IOT's Mobile Device Policy, the device must be enrolled in IOT's mobile device management platform MobileIron and the user must comply with the IOT Semi-managed BYOD Program policies and procedures.
 - 7.1. With the MobileIron app the user will be able to securely access their State Email, calendar and contacts.
 - 7.2. For devices for which the MobileIron app is not available or as an alternative means of access State Email, calendar, contacts, and other IOT-provided cloud services, the device's web browser can be used by going to <https://outlook.office365.com>; the user will need to be enrolled in IOT's multi-factor authentication service (<https://pfp.iot.in.gov/portal>) to use this alternative.

8. If possible, the number of email messages that may be retained on the device should be limited. This would help minimize any exposure should an unauthorized person somehow gain access to the device.
9. Downloading of State Email attachments to the device is generally prohibited, subject to procedure C below.
10. If the device is to be returned, sold, given away, or otherwise disposed of, all of the data on the device is to be permanently erased first. For state issued devices, IOT shall wipe all content prior to re-issuing the device. For non-state-owned devices, it is the user's responsibility to contact the IOT Help Desk to have the MobileIron administrator wipe all State information and applications from the phone; the user is to also permanently erase all of the data on the device (following the manufacturer's instructions for doing so) and to attest that they have done so.
11. If the device is not capable of meeting the standards in this section, the user is prohibited from using it to access any client personal information.
12. Non-state issued devices used to access client personal information under this section require written approval from the FSSA Privacy & Security Officer, excepting only personally-owned devices used as described in Procedure B below. Smart phones and tablets must be enrolled in the IOT MobileIron platform, as described above.
13. The user of the device is responsible for protecting any client personal information on the device from any form of unauthorized access (e.g. loaning device to others, adding inappropriate applications, etc.).

14. **Alert:** If the device is lost or stolen:

- 14.1. ***Immediately change your state network password***—the password you use to access your State Email Account and FSSA systems. You can use the Self-Service Password Management (SSPM) tool (if you have enrolled your account) provided by IOT or call the IOT Help Desk.
- 14.2. Notify your supervisor and your assigned Privacy/Security Liaison so that precautions can be taken to monitor any unauthorized attempts to access your State Email Account.
- 14.3. Call the IOT Help Desk to report the incident. For state-owned devices and for many personal devices, IOT can remotely wipe the device.
- 14.4. If it is your personal device, contact your carrier to report the incident; your carrier can disable the device so it cannot be used as a phone or to access the Internet.

B. Personally-owned **personal computers, smart phones, tablets**, and similar devices may be used to access State Webmail via the browser functionality of the devices (i.e., by accessing <https://outlook.office365.com> through the Internet, provided:

1. The device should be protected with a complex password, complex passcode, or biometric authenticator, and have up-to-date anti-virus and firewall technology employed as described above. The password/passcode should not be stored on or with the device.
2. Downloading of State Email attachments to the device is generally prohibited, subject to procedure C below.
3. If your personally-owned device connects to the Internet by way of a home wireless network (WiFi), your wireless network should be encrypted (WPA2 or greater) and password protected to prevent eavesdropping and unauthorized use of your wireless network.
4. Do not access State Webmail from public networks or hot spots—these are not secure—unless your device is enabled with and you are using a virtual private network (VPN).
5. The user will need to be enrolled in IOT's multi-factor authentication service (<https://pfp.iot.in.gov/portal>).
6. If the device is lost or stolen, follow the directions under A.12 above.

C. With respect to **downloading State Email attachments** containing client personal information to personally owned devices (smart phones, personal computers, tablets, notepads, etc.):

1. Client personal information cannot be stored on non-state-owned devices, subject to Policy #4 of this Section 7.
2. FSSA recognizes that periodically, when accessing State Email on a personal device it is necessary to download an email attachment to read it or work with it. In these situations:
 - 2.1. The attachment may be downloaded temporarily for immediate use.
 - 2.2. Upon completion, the downloaded attachment is to be immediately deleted (including from any recycle bin and download folders).
 - 2.3. Care should be taken to ensure that any downloads are not accessible by others who may otherwise have access to the device (e.g., family members). If necessary, this may require you to encrypt and password protect the document while it is on your device.
 - 2.4. The staff person is responsible to ensure the security and confidentiality of any attachments downloaded, including the introduction of a virus or other malware if any attachments are uploaded (e.g., you revise and email back a Word document; your anti-virus software should scan the document before uploaded to minimize the risk that a virus attached itself to your document).
 - 2.5. Care should be taken to avoid allowing files with client personal information from being automatically backed up to an unauthorized remote location, including cloud-based backup services and external back-up drives (i.e., auto backup utilities such as Carbonite should be turned off for files containing client personal information).

D. With respect to **portable media devices** (e.g., USB drives, external hard drives, CD/DVD's, tape):

1. Client personal information cannot be copied or transferred to any portable media except FSSA approved encrypted USB Drives and hard drives.
2. Copying or transferring client personal information should be limited to only when absolutely necessary for legitimate business purposes and then to the absolute minimum amount of information necessary for the business purpose.
3. Once the purpose for the copy or transfer is complete, the client personal information on the portable media should be completely erased.
4. The staff person copying/transferring the client personal information to the portable media is responsible for the security of the device, including the ability to completely replicate all of the client personal information should the device be lost or stolen.
5. Because the portable media is encrypted, each device must be set up with the appropriate security policies, including the use of a complex password or biometric authenticator.
 - 5.1. Each business unit is responsible for designating a staff member to serve as Administrator for the portable devices to order, inventory, setup (if necessary), and deploy the devices to the users.
 - 5.2. Only users with a legitimate business need for portable media should be provided with the device.
6. When portable media devices are no longer needed by a user, they are to be turned in to the designated business unit Administrator to be recycled, which will permanently erase all data on the device and make it available for reuse.
7. **All other portable media** (non-encrypted) in place at each business unit is to be promptly turned in to the FSSA Privacy & Security Office for proper destruction.

E. Laptop/Portable Media Backup:

1. As noted, staff members are responsible for the security of client personal information copied or transferred to laptops and portable media devices, including the ability to completely replicate all of the data on the laptop/device should the laptop/device be lost or stolen.
2. If the client personal information cannot be easily replicated from FSSA systems, the staff member should backup the client personal information on the device to their network “home” drive. This can be easily accomplished using Windows Explorer (copy or drag).
 - 2.1. If it is not possible or practical to back up the information to one’s “home” drive: for laptops, a backup may be made to approved (encrypted) portable media provided the portable media is secured (e.g., locked in a drawer) and kept separate from the laptop. For portable media, a backup may be made to a second approved portable media device, which is to be secured and kept separate from the first device.

- 2.2. Once the purpose for which the client personal information was copied to the device is complete, the client personal information should be appropriately filed for retention purposes and the copies on the devices shall be securely deleted.
- F. Under Policy #4 of this Section 7, client personal information cannot be copied or transferred to a laptop that is not encrypted.
- G. With respect to laptops:
1. Laptops should be physically secured when not in use (e.g. stored in a locked cabinet, cable locked if used in an area accessible to the general public, etc.). Contact the FSSA Privacy & Security Office for guidance on reasonable measures for securing laptops.
 2. Laptops should be physically secured during transport:
 - 2.1. Lock the laptop in the trunk of your car—don't leave it on the seat where it can be easily seen.
 - 2.2. When not in use, the laptop should be "screen locked" or powered down in a manner requiring entry of your password to gain access.
 - 2.3. Do not leave the laptop unattended during transport.
 - 2.4. Do not leave the laptop in your car (trunk or otherwise) overnight.
 3. Family members, friends, and others are strictly prohibited from using a state-owned laptop.
 4. FSSA staff are responsible for the security of any state-owned laptops they take offsite.
 5. If the laptop is lost or stolen, follow the instructions under A.12 above.
 6. If you are using a loaner laptop, prior to turning the laptop back in:
 - 6.1. Delete all client personal information from the laptop, including from the recycle bin and download folders.
 - 6.2. Have the administrator of the laptop remove you as a user (this removes your ID and your password from the laptop).

Section 8: Fax Policy Section

Purpose

Periodically, client personal information must still be faxed. The purpose of this policy is to ensure that faxing client personal information is kept to the minimum necessary and that any such faxing is appropriately secured.

Policy

With respect to faxing client personal information, whether faxed within the agency or outside of the agency, it is FSSA's policy that:

1. Faxing of client personal information should be avoided if possible; it is more secure to email the information following the rules established in [Section 6 Email Policy](#).
2. If faxing of client personal information is necessary, the procedures established in this policy are to be followed.
3. Under no circumstances is Federal Tax Information received by the agency from the Internal Revenue Service or the Social Security Administration to be faxed. Such information must be otherwise securely communicated (contact the FSSA Privacy & Security Officer for guidance). Inadvertent faxing of FTI must be reported as an incident in accordance with [Section 5.2](#) of these Privacy & Security Compliance Policies.

Procedures

If client personal information must be faxed:

1. The client personal information is to be limited to the amount minimally necessary for the purpose of the fax (minimum necessary rule applies).
2. The FSSA staff member faxing the client personal information must be authorized to see and use such information in accordance with the business unit's privacy policies and procedures.
3. A fax coversheet is to be used that contains:
 - a. The name, address, and phone number of the business unit sending the fax.
 - b. The name, telephone number, and fax number of the person sending the fax.
 - c. The total number of pages being faxed, including the cover sheet.
 - d. The date and time the fax is sent.
 - e. Any special instructions regarding the fax, such as special delivery instructions, the need for immediate attention, etc.
 - f. Instructions for the recipient to call the sender immediately upon receipt of the fax to confirm its receipt, including the number of pages received.

- g. Instructions for the recipient to clear any memory buffers in their fax machine or multi-function device (or delete from their fax server), if the machine is so equipped, so that the fax cannot be reprinted.
 - h. A warning banner across the top: *This fax contains confidential and privileged information.*
 - i. A Confidentiality Notice at the bottom: *This facsimile contains confidential and privileged information. If you have received this facsimile in error, please immediately call the sender and destroy all copies of the facsimile by shredding; clear any memory buffers on your fax machine or delete it from your fax server; and, do not copy or further transmit the facsimile.*
- 4. The person sending the fax is to call the recipient prior to faxing the client personal information so that the recipient is aware that the fax is being sent; and, to ask the recipient to call back the person sending the fax to confirm its receipt, including the number of pages sent.
- 5. Confirm with the recipient that the fax, including all pages sent, was received.
- 6. If a fax containing client personal information was inadvertently sent to the wrong recipient:
 - a. The sender should immediately call the recipient:
 - i. Explain the fax was sent in error;
 - ii. Request that the recipient shred the fax (all pages) and clear any memory buffers on their fax machine (or multi-function device) or delete from their fax server so that the fax cannot be reprinted; and,
 - iii. Obtain written confirmation (get the recipient's name, email, address, and phone number) that the fax was shredded, and the memory cleared from their fax machine (or deleted from their fax server).
 - b. The sender should report the incident in accordance with [Section 5.2](#) of these Privacy & Security Compliance Policies.

Alert: The person sending the fax is responsible to ensure the fax is sent in accordance with these procedures, including confirmation that the fax was completely received by the intended recipient.

With respect to client personal information received by fax (sent from within or outside of the agency):

1. The FSSA staff member receiving the fax must be authorized to see and use the client personal information (anticipated to be sent) in accordance with the business unit's privacy policies and procedures.
2. Request that the sender of the fax call you just prior to sending the fax.
3. Stand by the fax machine to ensure you are the only one to physically receive the fax.
4. Confirm the number of pages received matches the count provided by the sender.
5. Call the sender to confirm the receipt of the fax and the number of pages.
6. Clear the memory buffer of the fax machine, if it has one (refer to the machine's operation manual), or delete it from your fax server (if used) to ensure the fax cannot be reprinted.
7. Note on the fax cover sheet the date and time you called the sender and the date and time you cleared the fax machine memory buffer (if it has one; if it does not, make a note to that effect on the fax cover sheet).

Regarding fax machines with stored fax numbers (e.g., speed dial) or the use of fax servers with stored fax numbers:

1. The name of the recipient or organization associated with the fax number should be clearly identified.
2. The fax numbers are to be verified for correctness at least every three months; the business unit owning/using the fax machine is to create a log of each verification and retain it for one year.
 - a. Fax numbers can be verified by calling the recipient or organization associated with the fax number to confirm the number is still valid.
 - b. Changed or discontinued fax numbers should be corrected immediately on the fax machine or fax server.

Section 9: Computer & Paper & Media Disposal

Purpose

Proper disposal of computers, paper records, and other media that contains client personal information is essential to ensuring such information is completely eradicated as part of the disposal process; thus, avoiding any opportunities for a privacy/security incident to occur.

Policy

It is FSSA's policy that:

1. Each business unit will develop Computer & Paper & Media Disposal policies and procedures, and submit those to the FSSA Privacy & Security Officer for review and approval.
2. With respect to computers (desktops, laptops, tablets, and similar computing devices including state-owned smart phones), the business unit's policies and procedures should address:
 - a. Validating with the Indiana Office of Technology that all computers in use by their business unit have the appropriate encryption agent installed to protect client personal information.
 - b. Maintaining an inventory of such devices to be disposed of or put into surplus (e.g., asset tag number, description, date disposed of);
 - c. Sanitizing the memory and hard drives of the devices; this may include reliance on IOT for sanitizing⁷ devices;
 - d. Disposing of all such devices by returning the device to the Indiana Office of Technology (IOT) for proper sanitization and physical disposal (or reimaging and redistribution); and,
 - e. Specifically addressing such devices that are not going to be returned to IOT and how the devices will be sanitized and physically disposed of or sanitized and put into surplus.
3. With respect to paper disposal, the business unit's policies and procedures should address:
 - a. Establishing a retention schedule in compliance with relevant laws governing any client personal information maintained by the business unit.
 - b. A requirement to shred all paper documents that contain client personal information within the proper retention schedule;
 - i. A definition as to the type and degree of shredding (adhere to NIST 800-88 standards);
 - c. Provision of secure shred bins or baskets (e.g., locked), including distribution; and,

⁷ Sanitizing of hard drives and memory (where data is retained in memory) and media cards typically is to be done in conformance with the National Institute of Standards & Technology (NIST) Special Publication 800-88 Rev 1.

- d. A determination as to whether the business unit will perform the shredding or use a qualified third-party service, including the Indiana Archives and Records Administration shredding service (Business Associate Agreement required for third-parties).
- 4. With respect to electronic media (e.g., USB drives, CD/DVD's, tapes, external hard drives, etc.), the business unit's policies and procedures should address:
 - a. Sanitizing memory (e.g., USB drives) and hard drives prior to disposal or putting into surplus;
 - i. Keeping a log of all such devices sanitized and disposed of or put into surplus
 - ii. Sanitizing in conformance with NIST 800-88 Rev 1
 - b. Method of physical disposal or putting into surplus; and,
 - c. Means to thoroughly destroy media such as CD/DVD's and tapes, as part of the disposal process, such that any data that may be contained on the media is irretrievable.
- 5. With respect to microforms (e.g., microfilm, microfiche, etc.), the business unit's policies and procedures should address:
 - a. The method and means to securely collect microform media (e.g., use of locked burn bins); and,
 - b. The method and means to thoroughly destroy microform media (e.g., burn to white ash), including whether the business unit will engage a third party to perform the destruction (requires a Business Associate Agreement).

Procedures

As discussed above, each business unit is to develop Computer & Paper & Media Disposal policies and procedures and submit them to the FSSA Privacy & Security Officer for review and approval.

Advisory: All FSSA business units are strongly encouraged to turn into the FSSA Privacy & Security Office all CD/DVD's, tapes, unapproved USB drives, unused phone memory cards, and similar media as soon as possible for proper disposal. In accordance with [Section 7](#), only FSSA-approved portable media may be used; all other media will need to be sanitized and disposed of. The FSSA Privacy & Security Office will undertake the disposal effort for this media so the business units need not worry about the proper disposal of these legacy items.

If any of the unapproved media contains information the business unit needs to retain, the information first may be copied to an approved portable media device or to the network home drive of an authorized user prior to turn in.

Section 10: Training Requirements

Purpose

To assure continuing compliance with these Privacy & Security Compliance Policies & Procedures and to promote security awareness, all FSSA personnel, including embedded contractors, will receive training on these Privacy & Security Compliance Policies & Procedures and receive security awareness training. FSSA personnel with significant privacy and security responsibilities will also receive appropriate, role-based privacy and security training.

Policy

Privacy & Security Compliance Policies & Procedures Training

All FSSA personnel and embedded contractors are to be trained on these Privacy & Security Compliance Policies & Procedures. All new hires and transferees will be trained on these Privacy & Security Compliance Policies & Procedures within thirty (30) calendar days of their hire or transfer date. All FSSA personnel and embedded contractors, after initial training, will receive refresher training on these Privacy & Security Compliance Policies & Procedures at least once every 365 days and whenever there is a substantive change to these Privacy & Security Compliance Policies & Procedures.

The FSSA Privacy & Security Officer is responsible for developing training content, assuring timely training delivery to FSSA personnel and embedded contractors, and tracking training completion and staff acknowledgement.

All FSSA personnel and embedded contractors will acknowledge their participation in such training, their understanding of the training content and these Privacy & Security Compliance Policies & Procedures, and their agreement to comply with these Privacy & Security Compliance Policies & Procedures. The FSSA Privacy & Security Officer will maintain a record of FSSA personnel and embedded contractors training completion and acknowledgement. Failure to complete any required training may subject FSSA personnel to termination of account privileges as well as the State Personnel Progressive Discipline policies. Failure to complete any required training may subject embedded contractors to termination of account privileges as well as appropriate discipline as defined by the contractual agreements established with the vendor. These training records shall be maintained for at six (6) years beyond the date they were created.

Security Awareness Training

All FSSA personnel and embedded contractors are to receive security awareness training. All new hires and transferees will receive security awareness training within thirty (30) calendar days of their hire or transfer date. All FSSA personnel and embedded contractors, after initial training, will receive refresher security awareness training at least once every 365 days and whenever there is a substantive change to policies, procedures or systems that warrants additional or revised security awareness training.

The content of the security awareness training is determined by the FSSA Privacy & Security Officer and may be varied from time-to-time to address new types of security threats, new or revised methods of securing information systems and other resources, and to address system, business process, and regulatory changes. Basic security awareness training will address:

- The need for information security and actions necessary to maintain security and privacy of client personal information;
- Risks and threats, including insider threats, to information security and privacy;
- Threat identification techniques and reporting procedures;
- FSSA Security Policies (for awareness); and,
- Appropriate rules of behavior regarding the use of State Information Resources⁸.

The FSSA Privacy & Security Officer is responsible for developing training content, assuring timely training delivery to FSSA personnel and embedded contractors, and tracking training completion and staff acknowledgement.

All FSSA personnel and embedded contractors will acknowledge their participation in such training, their understanding of the training content and these Privacy & Security Compliance Policies & Procedures, and their agreement to comply with these Privacy & Security Compliance Policies & Procedures. FSSA Privacy & Security Officer will maintain a record of FSSA personnel security training completion and acknowledgement.

Role-based Training for Staff with Significant Privacy & Security Roles & Responsibilities

Privacy & Security Office Staff with Significant Privacy & Security Roles & Responsibilities:

The FSSA Privacy & Security Officer will develop, deliver, and track role-based security awareness training for FSSA Privacy & Security Office personnel with assigned privacy and security roles and responsibilities. This training will address the unique roles and responsibilities for such personnel. The FSSA Privacy & Security Officer will determine the appropriate training content and delivery mechanisms (and may supplement the training or employ third-party training opportunities as appropriate).

Such role-based training will be provided to appropriate FSSA Privacy & Security Office personnel new hires and transferees within thirty (30) days of their hire or transfer date; appropriate FSSA Privacy & Security Office personnel, after initial training, will receive refresher role-based training at least once every 365 days and whenever there is a substantive change to policies, procedures or systems that warrants additional or revised security awareness training.

FSSA Business Unit Staff with Significant Privacy & Security Roles & Responsibilities:

FSSA business units, as appropriate, will develop and deliver role-based security awareness training to its staff with assigned significant privacy and security roles and responsibilities (e.g., security coordinators, information technology staff).

Such role-based training will be provided by the business units to appropriate staff new hires and transferees within thirty (30) days of their hire or transfer date; appropriate staff, after initial training, will

⁸ The Information Resources Use Agreement (IRUA) training provided by IOT for all state workforce members provides the necessary rules of behavior training and acknowledgement and satisfies this training requirement; the FSSA Privacy & Security Officer and/or each business unit may require additional rules of behavior training and/or acknowledgement at their discretion.

receive refresher role-based training at least once every 365 days and whenever there is a substantive change to policies, procedures or systems that warrants additional or revised security awareness training.

Security Policy Awareness

The FSSA Security Policies are applicable to all FSSA business units. The Security Policies predominately apply to the development, deployment, and use of information systems. As such, most staff should be aware of the Security Policies (as provided in the Security Awareness Training); however, FSSA information technology staff (including appropriate vendors, contractors, and embedded contractors) should have a detailed understanding of the Security Policies. As such, the FSSA Privacy & Security Officer will conduct, from time-to-time and as needed or reasonably requested, physical or virtual work sessions to cover the Security Policies to provide a detailed understanding.

The FSSA Privacy & Security Officer will also publish the Security Policies on the FSSA Hub website and other venues as appropriate for use by interested and affected parties. Where applicable, compliance with the FSSA Security Policies will be incorporated into Business Associate/Vendor contracts.

The FSSA Security Policies are incorporated into these FSSA Privacy & Security Compliance Policies and Procedures by reference. As such, the FSSA Security Policies are included in the annual review (and updates as appropriate) of these Policies and Procedures by the FSSA Privacy & Security Officer.

Access to Federal Tax Information (FTI)

FSSA personnel that have authorized access/use of Federal Tax Information (FTI) provided to the agency by the Internal Revenue Service (IRS) or the Social Security Administration (SSA) are to be provided specific FTI awareness training regarding the protection of FTI and the sanctions for misuse of FTI. This training must be completed prior to the agency granting authorized personnel access to FTI. Note, for human services agencies (e.g., FSSA) only state employees are permitted access/use of FTI under federal law.

It is the responsibility of each business unit that receives FTI from the IRS to identify who within the business unit is to have authorized access/use of such FTI, ensure such staff receive the appropriate FTI awareness training prior to be granted access, obtain certification from such staff that they have received the training and understand their responsibilities for safeguarding the FTI and the sanctions for misuse, assure such training and certification occur at least once every 365 days, and keep a record of such training and certification for no less than six (6) years. It is also the responsibility of the business unit to ensure this training meets the requirements under IRS Publication 1075.

Note: certain training programs that meet the IRS training requirements are available from the IRS Office of Safeguards.

Training Records

FSSA shall retain individual training records for six (6) years. FSSA training records shall track both Privacy & Security Compliance Policies & Procedures training and security awareness training and specific, targeted or specialized security training provided.

All individual training records—training type, trainee, date completed, acknowledgment obtained—shall be retained for six (6) years.

For FSSA Privacy & Security Compliance Policies & Procedures Training and Security Awareness Training, the FSSA Privacy & Security Officer will retain (or cause to be retained) the training records.

For role-based training of FSSA Privacy & Security Office staff with significant privacy and security roles and responsibilities, the FSSA Privacy & Security Officer will retain the training records.

For role-based training of business unit staff with significant privacy and security roles and responsibilities, the business unit is responsible to retain the training records.

For security policy awareness work sessions (conducted by the FSSA Privacy & Security Officer for individuals requiring a more detailed understanding of the security policies), specific training records need not be retained; however, it may be advisable for the FSSA Privacy & Security Office to record when such sessions are provided, including a list of the attendees.

For FTI training, it is the responsibility of the associated business unit to retain the training records.

Training Materials Review

Training materials are to be reviewed by the responsible party no less than every 365 days to assure continued accuracy, relevance, and applicability. The responsible party will maintain a log of its review of the training materials review, including an annotation as to whether updates were made.

Training materials will be updated by the responsible party whenever substantive changes occur to policy, procedure, systems, regulatory requirements, or other changes that affect the content of the training.

Responsible parties are:

- FSSA Privacy & Security Officer:
 - FSSA Privacy & Security Compliance Policies & Procedures
 - Security Awareness Training
 - FSSA Privacy & Security Office staff role-based privacy/security training
- Business Unit (as applicable):
 - Privacy/Security Role-based training
 - FTI training
 - Business Unit policy/procedure training
 - Any other applicable privacy/security training deemed appropriate by the business unit

All business unit personnel will be trained on the business unit's subsidiary policies and procedures within a reasonable timeframe established by the business unit.

Procedures

The FSSA Privacy & Security Officer will determine the most appropriate procedures for providing the required training. The objective will be to provide a training curriculum and delivery method most suitable to effectively reach all FSSA personnel within the required timeframes. The FSSA Privacy & Security Officer will develop, to the extent needed, more detailed procedures on training content development, deployment, and competency exams.

Embedded Contractors

As defined in these policies and procedures, workforce members are state employees, volunteers, interns, trainees, contractors (engaged by the IDOA Managed Service Provider; also referred to as contingent labor), and other persons whose conduct, in the performance of work for FSSA, is under the direct control of FSSA, whether or not they are paid by FSSA. All workforce members, including contingent labor contractors, are subject to FSSA's policies and procedures, including the training requirements outlined in this section.

An example of a contingent labor contractor, as used here, would be a security analyst engaged by the FSSA Privacy & Security Office (usually at an hourly rate) who works under the direction of the FSSA Privacy & Security Officer, whether or not the contractor is an independent or is employed by a third party.

Certain vendors, however, are not under the direct control of FSSA with respect to the performance of their daily work (i.e., are not contingent labor). For these vendors, performance metrics and deliverables are established in a contract between the vendor and FSSA. Provided the vendor does not use FSSA and/or State Information Systems in the performance of their services to FSSA (excluding email), then these vendors are not typically subject to FSSA's policies and procedures.

Other vendors, referred to here as embedded contractors, while not typically under the direct control of FSSA with respect to the performance of their daily work, use FSSA and/or State Information Systems in the performance of their services to FSSA. Embedded contractors are subject to FSSA's policies and procedures because they use state systems.

As such, embedded contractors are to be trained on FSSA's Privacy & Security Compliance Policies & Procedures and undergo security awareness training as described in this section.

The FSSA Privacy & Security Officer may adjust the training materials to reflect certain differences between embedded contractors and workforce members, as he/she may deem appropriate. In addition, the FSSA Privacy & Security Officer may, at his/her discretion, require to embedded contractor to provide the mechanisms to deliver the training to its staff, track such training in accordance with this section, and retain the training records in accordance with this section—the embedded contractor will provide copies of the training records to the FSSA Privacy & Security Officer upon request.

In order to verify which specific training is necessary for a contracted resource, intern, and/or volunteer, the FSSA business unit should contact the FSSA Privacy & Security Office for guidance.

Section 11: Staff Protection from Retaliatory Acts

Purpose

One objective of this policy is to help ensure that any known or suspected privacy/security incidents are promptly reported. Staff personnel must be assured that if they report a known or suspected privacy/security incident they will not be subjected to any form of retaliatory act or disciplinary action by FSSA or the state.

Policy

It is FSSA's policy that the agency, including its management and staff, will not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any member of FSSA's workforce who has reported a known or suspected privacy/security incident or has exercised any rights under the applicable federal and state laws and regulations (under which these Privacy & Security Compliance Policies were developed). Such retaliatory acts are a direct violation of this policy.

This policy does not prevent FSSA from undertaking appropriate disciplinary action for policy violation(s) by a staff person reporting a suspected or known privacy/security incident.

Procedures

1. If any member of FSSA's workforce believes they have been retaliated against, regardless of form, for reporting a known or suspected privacy/security incident, the staff person should immediately notify their supervisor, unless the supervisor is the alleged source of the retaliation in which case the staff person should report the situation to the FSSA Human Resources Director.
 - 1.1. If, after reporting an alleged retaliation to their supervisor the staff person believes the supervisor has not acted on the report in good faith or in a timely manner, the staff person should contact the FSSA Human Resources Director.
2. The staff person's supervisor, in collaboration with the FSSA Human Resources Director, will promptly investigate the alleged retaliation and report the results to the FSSA Human Resources Director.
 - 2.1. If appropriate, the Human Resources Director will undertake the investigation.
3. The FSSA Human Resources Director will respond to the results of the investigation in accordance with FSSA's policies for dealing with policy violations, including the imposition of sanctions on those responsible for the retaliatory acts.

Section 12: Sanctions for Policy Violation

Purpose

It is the purpose of this policy to establish the sanctions FSSA personal are subject to for violation of these Privacy & Security Compliance Policies and Procedures.

Policy

Failure by FSSA staff to comply with these Privacy & Security Compliance Policies and Procedures, including any supplemental policies established by FSSA regarding the privacy and security of client personal information in FSSA's safekeeping and any subsidiary policies and procedures established by a FSSA business unit will be addressed using the State Personnel Department Progressive Discipline Policy and/or agency specific policy.

Those authorities prescribe the procedures for investigation, standards for decision making, and process for third party review of outcomes. Determinations of the severity of misconduct (categorization as minor, serious, or severe) will include consideration of factors identified in the state and federal laws identified within these policies (e.g., severity, intent, and patterns). Sanctions for contracted staff will be based on the provisions indicated in the applicable contracts and/or agreements.

Any use or disclosure of client personal information that is inconsistent with these Privacy & Security Compliance Policies and Procedures, any supplemental policies established by FSSA regarding the privacy and security of client personal information in FSSA's safekeeping and any subsidiary policies and procedures established by a FSSA business unit will be reported to the applicable Privacy/Security Liaison and/or the FSSA Privacy & Security Officer as defined in Section 5 of these Privacy & Security Compliance Policies and will be investigated as described therein.

FSSA personnel should also understand that in addition to any sanctions that may be imposed under this policy, the individual may also be subject to criminal and civil penalties as prescribed under applicable state and federal law.

Procedures

None under this policy.

Section 13: Retention Policy

Purpose

FSSA is obligated under both state and federal laws and regulations to maintain certain documentation regarding client personal information for specified periods of time (e.g., FSSA records retention schedule, Indiana Archive and Records Administration, HIPAA Privacy Rules, etc.).

Policy

All actions and activities under these Privacy & Security Compliance Policies will be documented and retained in accordance with applicable retention laws and regulations, but in all cases for no less than six (6) years from their date of creation. Each version of these Privacy & Security Compliance Policies will likewise be retained for a period of no less than six (6) years from its creation date.

The individual business units are responsible to retain copies of their subsidiary policies and procedures in accordance with applicable retention laws and regulations, but in all cases each version must be retained for no less than six (6) years from its creation date.

The FSSA Privacy & Security Officer is responsible for maintaining all documented actions and activities (e.g., Incident File) under these Privacy & Security Compliance Policies for the required timeframe and in a manner that allows for reasonable, timely retrieval.

Procedures

The FSSA Privacy & Security Officer will develop procedures for the Privacy & Security Office to document and maintain these Privacy & Security Compliance Policies and all actions and activities under these Privacy & Security Compliance Policies in a manner consistent with this policy.

Section 14: Federal Tax Information Background Checks

Purpose

The purpose of this policy is to define and establish procedural guidelines, background checks, and suitability standards for applicants, employees, and contractors who may have access to Federal Tax Information as part of their job duties with FSSA. IRS Publication 1075 requires that FSSA create a written policy that ensures compliance with IRS standards for persons having access to Federal Tax Information (FTI).

Policy

FSSA is committed to protecting its information, particularly its FTI. FSSA workforce members and/or contractors are not permitted to access or request tax payer information of any type from any Department of Revenue or federal Internal Revenue Service information system unless they have a lawful job-related reason for accessing such information. Upon being approved to handle FTI, workforce members will be required to maintain safeguard procedures as established by FSSA and the IRS. Workforce members will be required to have background checks and a suitability review every five (5) years.

Definitions

- A.** Background Check means all necessary checks required in order to have access to FTI. IRS Pub 1075 requires that checks must include, at a minimum, fingerprint checks (as permitted by the FBI), local law enforcement checks, and citizenship verification.
- B.** Citizenship Requirement Check means a subject's eligibility to legally work in the United States. Utilizes Form I-9.
- C.** Federal Tax Information (FTI) consists of tax returns and tax return information. FTI can be either or both. FTI is any return or return information received from the IRS or an IRS secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement, Bureau of Fiscal Services, or the Center of Medicare and Medicaid Services. FTI is also shared under agreements allowed by statute or regulations.
- D.** Fingerprinting means fingerprint background checks, as permitted by the FBI.
- E.** Local Law Enforcement Check means checks at local law enforcement agencies where the subject has lived, worked, and/or attended school within the past five years. These may include searches of the Indiana Data and Communications System (IDACS) and the National Crime Information Center (NCIC), as permitted by applicable laws.
- F.** Suitability Standards means agency criteria for determining a subject's suitability to have access to FTI. Suitability is a person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the efficiency and security of FSSA and its use and storage of FTI.

Relevant Law and Federal Guidelines

- A.** IRS Publication 1075, September 2016 Revision is a publication issued by the IRS that gives detailed requirements for governmental agencies and their employees that have access to FTI. This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of FTI.
- B.** 5 CFR 731.201 is a federal regulation utilized by the IRS for determining Suitability Standards for applicants, appointees, and employees. Many of the Suitability Standards used by FSSA are adapted from this regulation.

Procedure

- A. Background Check Requirements.** These requirements are conducted in conjunction with both state and federal agencies. In coordination with the Indiana State Personnel Department, it is the duty of the FSSA business units that handle FTI to ensure that all necessary steps have been completed before a subject is allowed access to **FTI**.
 - 1. Process.** **FTI** access requires that a subject pass the following checks:
 - a.** Fingerprinting, as permitted by the FBI
 - b.** Citizenship Requirement Check to verify eligibility to legally work in the United States
 - c.** Criminal History Check where the individual has lived, worked, and/or attended school within the last five (5) years
 - 2. Timeframe.** FSSA will conduct all Background Checks in a timely manner. The subject will not be allowed access to FTI until they have passed all Background Checks and have received a favorable rating under FSSA's Suitability Standards.
 - 3. Suitability Standards.** FSSA will consider the following crimes (federal or state equivalent) and activities in determining an individual's suitability to access **FTI**:
 - a.** Theft;
 - b.** Larceny;
 - c.** Burglary;
 - d.** Robbery;
 - e.** Fraud;
 - f.** Identity Theft;
 - g.** Illegal Credit Card Use of Another;
 - h.** Any crime involving fraud, deceit, or dishonesty with a potential for financial gain to the individual or for the benefit of another;

- i. Any crime with a direct link to the individual's specific job functions;
 - j. Material or intentional false statement, deception or fraud in examination or appointment; or
 - k. Any statute or regulatory bar which prevents the lawful employment of the person involved in the position in question.
 - 4. FSSA must consider any of the following additional considerations to the extent FSSA deems any of them pertinent to the individual case:
 - a. The nature of the position for which the person is applying or in which the person is employed;
 - b. The nature and seriousness of the conduct;
 - c. The circumstances surrounding the conduct;
 - d. The recency of the conduct;
 - e. The age of the person involved at the time of the conduct; and
 - f. The absence or presence of rehabilitation or efforts towards rehabilitation.
 - 5. **For Workforce Members Currently in Positions that Require Access to FTI:** The appointing authority or designee shall have discretion on retention decisions for any employee, contractor or sub-contractor who has been found guilty of any of the crimes or activities listed above, or similar crimes or activities, based on the age and circumstances of the underlying events leading to the guilty finding. Current employees must comply with investigation requirements, and revocation of access to FTI may result in dismissal.
 - 6. **For Workforce Members under Consideration for Hire in Positions that Require Access to FTI:** The appointing authority or designee shall not employ or contract with any person who has been found guilty of any of the crimes or activities listed above, or similar crimes or activities, within the last three (3) years. For guilty findings older than three (3) years, the appointing authority or designee shall have discretion on hiring decisions based on the age and circumstances of the underlying events leading to the guilty finding.
- B. Re-investigation Check Requirements.** IRS Pub 1075 requires that a reinvestigation of workforce members must be conducted every five (5) years from the date of the previous background investigation for each employee and contractor having access to FTI. Re-investigations will encompass the full five (5) year period.
- C. Safeguard Requirements.** The following FSSA policies apply to the security of FTI documents:
- 1. Access control policy
 - 2. Application security policy
 - 3. Audit and accountability policy
 - 4. Configuration management policy
 - 5. Contingency planning policy

FSSA Privacy & Security Compliance Policies & Procedures

6. Identification and authentication policy
7. Information security policy
8. Integrity policy
9. Maintenance policy
10. Privacy & Security Compliance Policies
11. Security assessment policy
12. Security planning policy

D. Workforce Member Reporting Requirements: it is the workforce member's duty to notify their Supervisor and HR representative of any of the following:

1. There have been changes in the workforce member's suitability to access FTI
2. Unauthorized personnel gained access to FTI

Section 15: Additional Privacy & Security Compliance Policies

Purpose

The purpose of this section is to incorporate additional Privacy & Security Policies & Procedures pertinent to FSSA and in compliance with associated federal and state laws and regulations, as well as, in compliance with applicable standards adopted by the agency or the state.

Policies

Artificial Intelligence (AI)

AI technologies have significant potential to transform society and people's lives. AI technologies, however, also pose risks that can negatively impact individuals, groups, organizations, communities, society, etc. Thus, any FSSA business unit that plans to implement or utilize any 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) established by IC 4-3-26-9 prior to the initiation of implementation activities.

Insider Threat

It's the responsibility of all FSSA business units to establish a procedure to mitigate the potential risk to sensitive information and/or systems that may be caused by FSSA Workforce Members under their supervision. This procedure should include a process to detect, prevent, and respond to threats posed by FSSA Workforce Members who may directly or indirectly have access to sensitive information and/or systems.

Publicly Accessible Content

Public information available from the Family and Social Services Administration (FSSA) on the website or other public accessible systems, shall not contain any confidential information, including, but not limited to personal information from clients or other individual private content.

It is the responsibility of authorized FSSA staff and business units to:

- Identify individuals authorized to post information onto public information systems;
- Train such individuals to ensure publicly accessible information does not contain non-public information;
- Review the proposed content for public information systems to ensure non-public information is not included; and,
- Complete periodic reviews of the content of the public information systems for non-public information, based on the volume of submissions to the FSSA websites, and remove such information if discovered; and to document the content review process.

Risk Assessments

All business units that have access to CPI are required to complete periodic risk assessments to confirm the proper controls are in place to protect this sensitive information. FSSA business units shall consult with the FSSA Privacy & Security Office to determine the appropriate scope, methods, and frequency for completing these required risk assessments.

Workforce & Data System Screening

The Indiana State Personnel Department is responsible for conducting workforce screening prior to employment or engagement in accordance with state personnel policy. FSSA data systems maintain a significant amount of sensitive data on the clients we serve. FSSA is subject to multiple federal laws that require our agency to implement security controls to protect the confidentiality, integrity and availability of this sensitive client data. These federal laws mandate that we conduct appropriate screening processes, including potential rescreening as appropriate, for any individuals who are granted access to sensitive FSSA client data. As such, all FSSA workforce members, contractors, and former state employees employed by external partners and/or contractors, who require access to sensitive FSSA client data are subject to screening processes established by the applicable FSSA business unit and/or the FSSA Privacy & Security Office. The screening processes utilized for access to FSSA data systems will be commensurate to the sensitivity level of the data being accessed.

Workforce Risk Designations

To the extent necessary and applicable, FSSA business units will establish criticality/risk designations to their organizational positions relative to the access to and use of client personal information; in particular, this would relate to role-based access privileges identified (reference Section 1 of these policies and procedures) and the assignment of personnel to such roles. When established, such role-based access privileges and personnel assignments will be reviewed no less than every 365 days to ensure the criticality/risk designations of the roles continue to reflect business unit requirements and the assignments remain appropriate.

Workforce Transfers/Separations

It is the responsibility of the FSSA business unit and the individual's direct supervisor to ensure that a FSSA workforce member's access to client personal information in all forms (e.g. network shares, SFTP sites, portable devices, applications, etc.) is immediately terminated upon the workforce member leaving the agency or upon transfer to another business unit or state agency. The business unit/supervisor will notify FSSA Account Control within one (1) business day, or immediately in urgent situations, of the individual's termination or transfer to assure timely disabling of the individual's access privileges. The direct supervisor is responsible for validating that all keys, access badges, laptops, smart phones, any client files (either paper or electronic), etc. are returned by the workforce member prior to leaving on their last day of employment. **Under no circumstances may any FSSA workforce member take any client files (either**

paper or electronic) with them as they separate employment from FSSA. The direct supervisor is responsible for validating that any client personal information is secured upon return (e.g. securely wipe laptops, smart phones, portable drives, etc.) by the workforce member.

If an individual will be temporarily separated from the agency (e.g., extended leave of absence), the business unit/supervisor is responsible to notify their HR representative, FSSA Account Control and FSSA Facility Management to temporarily suspend the individual's access privileges to systems and buildings.

With respect to embedded contractors, the contracting vendor is responsible to notify the FSSA business unit's contracting officers (or designees) of any personnel changes (transfers/terminations of vendor personnel assigned to FSSA) within one (1) business day of such changes. The methods and means of such notification will be determined between the vendor and the FSSA business unit.

Working Remotely

It is the responsibility of FSSA Workforce members (hereafter referred to as "Authorized Users") with remote access privileges to the State's network to ensure that their remote access connection is given the same consideration as the user's on-site connection. Authorized Users are responsible for preventing access to any State computer resources or data by non-Authorized Users. Performance of unauthorized activities through the State network by any user (Authorized or otherwise) is strictly prohibited.

It is the responsibility of Authorized Users to ensure the following:

- Remote WIFI networks used to connect to the State Network shall be encrypted and protected with a complex password.
- Any personal devices used to connect to the State Network shall be protected by a complex password or biometric authenticator.
- Confidentiality of CPI shall be maintained by not permitting access by family, friends, and/or other non-authorized users.
- Establishing a secure remote workspace by taking reasonable measures to mitigate the risk to CPI (e.g. utilizing a low traffic area, locking devices when not in use, secure physical data such as paper files in a locked cabinet, etc.).
- Personal devices used to connect to the State Network shall have up to date anti-malware, the latest and appropriate firewalls enabled. Routine malware scans shall be performed with an anti-malware tool and any vulnerabilities that are identified must be addressed promptly.
- Personal devices used to connect to the State Network shall have up to date Operating Systems.
- Any web browsers used to connect to the State Network shall be current (e.g. latest version to mitigate any security vulnerabilities).
- CPI shall not be stored on any personally owned devices.
- CPI shall not be stored on any unauthorized cloud services (e.g. Google Drive, iCloud, Dropbox etc.).
- Storage of sensitive files on state owned devices including but not limited to CPI, shall be stored securely with the use of encryption and complex passwords.

FSSA Privacy & Security Compliance Policies & Procedures

- Creating physical copies of CPI documentation shall be avoided and/or minimized when possible. If there is a legitimate business need for printing, the following controls must be considered:
 - Verify that the printer is securely connected (e.g. hard-wired method) to the personal device.
 - Verify that the printer is located in a reasonably secure location in your remote working space and that documentation is recovered promptly by the Authorized User (e.g. low traffic areas, secure area where others have limited or no access).
 - Printer drivers and software are up-to-date.
 - Verify that documents are not saved locally on printers with internal storage.
 - Securely shred any documents containing CPI upon completion of the business need and/or function.
- Any personal devices (e.g. hard drives, computers, phones) shall be securely wiped (e.g. format drives) prior to the disposal or transfer of the device.
- A minimum necessary approach shall be utilized when CPI is involved for any business needs and/or functions.

Section 16: Definitions

These definitions apply to these Privacy & Security Compliance Policies and Procedures.

Term	Definition
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.
Breach	This term breach has a particular meaning under the HIPAA Breach Rule: the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rules which compromises the security or privacy of the protected health information. Under these Privacy & Security Compliance Policies, this definition is expanded to include all client personal information in FSSA's safekeeping in which an improper disclosure of client personal information has occurred in violation of these policies, business unit policies, state security policies, and/or applicable federal and state laws and regulations. Under the HIPAA Breach Rule, <u>a breach requires written notification to the victim</u> of the breach (the person whose PHI was improperly disclosed). Under these Privacy & Security Compliance Policies, the requirement is expanded include breaches of any client personal information in FSSA's safekeeping. In addition, certain state laws and administrative codes require written notice to the victim of a breach of confidentiality (e.g., IC 4-1-11 requires notice to the victims of a security breach; IAC 5-1-1 requires notice to victims for which their social security number is disclosed in violation of IC 4-1-10). Thus, the expansion of the definition of a breach under these Privacy & Security Compliance Policies helps to assure FSSA's compliance with state laws and regulations. The HIPAA Breach Rule allows for certain exclusions in which an improper disclosure is not considered a breach; for example, unintentional access otherwise made in good faith or a disclosure in which there is reasonable belief that the

FSSA Privacy & Security Compliance Policies & Procedures

		recipient could not have retained the client personal information. The FSSA Privacy & Security Officer will consider these exclusions as guidance, in addition to guidance provided by other sources such as the Office of the Indiana Attorney General, with respect to making a determination as to whether a privacy/security incident has resulted in a breach. With respect to certain federal agency reporting of breaches (e.g., SSA, IRS, CMS), the term breach is further defined as: the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Business Associate		A Business Associate (BA) is a person or entity that performs a service for FSSA and within the scope of that service obtains, creates, maintains, or uses client personal information—specifically, protected health information. BA's are under contract with FSSA and the contract has specific provisions regarding the BA's obligations with respect to the client personal information, including PHI. Individual contractors acting as a member of FSSA's workforce may not necessarily be BA's, but are still obligated to comply with these Privacy & Security Compliance Policies and all applicable laws and regulations protecting client personal information.
Business Unit(s)		Business unit means, collectively and individually, FSSA divisions, bureaus, sections, facilities (including State Operated Facilities, or SOF's), and program areas. This is a term of convenience. For example, the Division of Family Resources is a business unit; the Bureau of Child Care is a business unit within the Division of Family Resources business unit.
Client		Means constituents, beneficiaries, applicants, patients, customers, members, and other terms used by FSSA's various programs to describe individuals who have <u>applied for and/or are the recipients of FSSA services</u>. This includes information on former clients (applicants, beneficiaries, etc.) whose information remains in FSSA's safekeeping. Use of the term client is intended to simplify policy and procedure statements by having a single reference term.

Client Personal Information (CPI)		Means Personal Information about a client.
Complex Passcode		Complex Passcodes apply to smart phones, tablets, and similar devices that employ a numeric passcode instead of a password. A Complex Passcode must be at least six (6) digits in length and not easily guessable. For example, not be 1-2-3-4-5-6, 5-5-5-5-5-5, 7-4-1-3-6-9, etc. To be secure, the device must be set to lock the device after no more than 10 invalid passcode entry attempts.
Complex Password		In accordance with IOT Tier 1 Security Standard IOT-CS-SEC-117, a complex password is: 1. A password that contains at least eight (8) characters; and, 2. A password that contains characters from three of the four following categories: 2.1. English uppercase letters (A-Z) 2.2. English lowercase letters (a-z) 2.3. Base ten digits (0-9) 2.4. Special characters (\$, #, %, *, _, etc.) Certain FSSA information systems require a complex password that requires characters from all four of the above categories and requires expiration every 60 days. The use of two-factor authentication—for example, use of biometrics and a PIN—instead of a complex password requires written permission of the FSSA Privacy & Security Officer. A complex password for Microsoft Office files shall include: a. At least sixteen (16) characters; b. Characters from at least three of the following four categories: i. English upper case (A – Z) ii. English lower case (a – z) iii. Base ten digits (0 – 9) iv. Special characters (\$, #, %, *, _, etc.)
Covered Entity		A Covered Entity is an entity that must comply with the HIPAA rules. HIPAA defines a Covered Entity as a health plan, a health care clearinghouse, or a health care provider who transmits in electronic form any of the transactions covered under HIPAA (e.g., claims).

FSSA Privacy & Security Compliance Policies & Procedures

		Under the HIPAA rules, state Medicaid plans are specifically identified as Covered Entities. Much of FSSA falls within the definition of a Covered Entity.
Disclosure		As used in these Privacy & Security Compliance Policies, Disclosure means to provide client personal information to someone or some entity. Proper disclosures occur all of the time in the course of the agency's business. We disclose to providers that a client is eligible for medical services covered under their Medicaid plan; we disclose client case information to the client regarding their benefits status; we disclose client personal information to one another as part of our day-to-day jobs. Improper disclosures occur when we disclose client personal information to someone or some entity who is not authorized to have the information; a disclosure that is not permitted by these Privacy & Security Compliance Policies and the laws and regulations under which they were developed (e.g., HIPAA Privacy).
Embedded Contractor		Certain vendors, referred to here as embedded contractors, while not typically under the direct control of FSSA with respect to the performance of their daily work, use FSSA and/or State Information Systems in the performance of their services to FSSA. Embedded contractors are subject to FSSA's policies and procedures because they use state systems.
Encryption		Encryption makes words, documents, files, and email indecipherable to anyone who might see the information, unless they have the decryption key. The purpose is to prevent an unauthorized person from seeing the content. For example, say you want to send the message, "How are you, today?" Anyone who can see your message can see exactly what you wrote. However, if you encrypt the message, the reader would only see "ch& 99! Oh% 7h\$9O," unless they have the key to decode the message.
Encryption Standards		The encryption standards for portable devices approved by FSSA are those consistent with NIST Special Publication 800-111 <i>Guide to Storage Encryption Technologies for End User Devices</i>. The encryption standards for data in motion (transit) are those that comply with FIPS (Federal Information Processing Standards) 140-2, which includes, as appropriate, NIST

FSSA Privacy & Security Compliance Policies & Procedures

		Special Publication 800-52, <i>Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations</i>; 800-77, <i>Guide to IPsec VPNs</i>; or 800-113 <i>Guide to SSL VPNs</i>; and, may include others that are FIPS 140-2 validated. At a minimum, encryption technology employed by FSSA, including contractors to FSSA, will meet or exceed the encryption functionality for both data at rest and data in motion employed by IOT.
HHS		U.S. Department of Health and Human Services (HHS), which is the parent agency of the Centers for Medicare and Medicaid Services (CMS) and the Office of Civil Rights. HHS has ultimate responsibility for the development, promulgation, and enforcement of the HIPAA rules, as well as the regulations regarding Medicaid programs.
HIPAA		Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191). As a federal law, HIPAA has several components. For the purposes of these policies, we mean Title II, Subtitle F of the Act, which addresses Administrative Simplification. This section, among other things, provides the legal basis for the HIPAA Privacy Standard (or Rule) and the HIPAA Security Standard (or Rule), as well as the standards regarding HIPAA Compliance and Enforcement, and Civil Penalties (for failure to comply). Reference 45 CFR Parts 160, 162, and 164). HITECH supplemented HIPAA with, among other things, the HIPAA Breach Standard (or Rule). The HIPAA Act, as supplemented by HITECH, updated the Social Security Act, including Sections 1176 and 1177, which establish both civil and criminal penalties for HIPAA violations (the former for failure to comply with HIPAA, the latter for misuse of client personal information).
HITECH		In February, 2008 Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act (ARRA). Subtitle D of HITECH strengthened some of the provisions of the HIPAA Privacy Rule, ensured Business Associates are covered by HIPAA Privacy/Security, expanded enforcement capabilities, and increased the monetary penalties for failure to comply and the criminal penalties for abuses of protected health information.
Improper Disclosure		This is a disclosure of client personal information to people or organizations not authorized by policy or law to receive such information, including the disclosure of client personal

FSSA Privacy & Security Compliance Policies & Procedures

		information in violation of applicable laws and regulations, these Privacy & Security Compliance Policies, business unit policies, and/or state policies. For example, under HIPAA PHI cannot be disclosed to a state legislator unless the client has expressly authorized the disclosure.
Incident File		An electronic file, organized by privacy/security incident, maintained by the FSSA Privacy & Security Officer that contains all of the pertinent information regarding any given privacy/security incident. A secured paper file may also be maintained. The FSSA Privacy & Security Officer will securely maintain only the minimum amount of CPI necessary in the incident file. Incident Files are securely maintained under the direct control of the FSSA Privacy & Security Officer.
Incident Report		This refers to the official Incident Report prepared by the FSSA Privacy & Security Officer (or their delegate) regarding known and suspected privacy/security incidents. The objective of the report is to capture all of the pertinent details regarding a reported privacy/security incident and the conclusion drawn from the evidence (e.g., whether a reportable breach of confidentiality has occurred). Attached by reference to the report is all of the supporting information regarding the incident such as copies of emails about the incident, copies of the client personal information improperly disclosed or compromised, copies of notices (to the victims), and a list of all personnel involved in the incident. Multiple Incident Report forms are used, depending on the type of incident. The Privacy & Security Officer is responsible to maintain the Incident Report forms and preparation guidance.
Insider Threat		The potential threat that an FSSA Workforce Member will use her/his authorized and/or unauthorized access, wittingly or unwittingly, to do harm to the security of the FSSA data and/or systems. This threat can include damage to FSSA data and/or systems through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of FSSA resources or capabilities.
Multi-Factor Authentication (MFA)		This is a security measure also referred to as Phone Factor that will help validate your identity and secure state resources when accessing them off the state network. Logging into a cloud resource will require a valid username

		and password followed by a secondary verification to complete the login process. The secondary verification can be one of the following: • System-generated phone call that must be answered by the user with a valid response. • Text message sent to the user with a code that will need to be entered to complete the login process. • Installation of an authentication app on a smartphone that will require the user to accept or decline the authentication request. To access resources such as State Webmail, SharePoint Online, CRM Online, etc., from outside of the state network, users will need to enroll in MFA. Log in using your UPN (full email address) along with your network password.
OAG		Office of the Indiana Attorney General.
OCSE		Office of Child Support Enforcement. OCSE is part of the federal Health & Human Services (HHS) Administration for Children and Families (ACF).
OCR		Office of Civil Rights (OCR). OCR is a division of HHS and is directly responsible for the development, promulgation, and enforcement of the HIPAA Privacy, Security, and Breach rules.
Personal information		With respect to these policies, is the same as Client Personal Information. This is information about an individual, including health information. This is information that identifies the individual (e.g., name) and something about the individual (e.g., address, date of birth, gender, etc.). Certain types of client personal information are protected under state or federal law: PHI, PII, FTI. Client personal information includes information regarding an individual's legal guardian, authorized representative, family members, assistance group members, health care representative, provider, and other people directly associated with the individual. Client personal information may be in any form: electronic, paper (including microforms and similar media), or within verbal communications.

Personally Identifiable Information—PII	This is information associated to an individual; also referred to as PI or client personal information or Protected Information. Under IC 4-1-6 PI means any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual (e.g., education, financial transaction, medical history, employment records, photographs, etc.). Under IC 4-1-11, PI means an individual’s first name and last name or first initial and last name; and, at least one of the following: (a) social security number; (b) driver’s license number or identification card number; or (c) account number, credit card number, debit card number, security code, access code or password of an individual’s financial account. As defined by National Institute of Standards and Technology (NIST) Special Publication 800-122, <i>Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)</i>, “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information
Portable Media	This term refers the electronic media that can be used to store information including, but not necessarily limited to: USB drives, external hard drives, CD’s, DVD’s, tape, and smart phones that can also be used as USB drives.
Privacy/Security Incident	A privacy/security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of client personal information (CPI) or interference with system operations in an information system. Examples include (but are not limited to): • An email containing CPI is sent outside of the state network (e.g. any address not containing an fssa.in.gov extension) and is not encrypted using a approved tool —this could lead to attempted or successful unauthorized access to the information.

	• An appeal hearing packet is mailed to the wrong person—this could result in the disclosure of CPI to an unauthorized person. • A laptop containing or potentially containing client personal information is stolen—the thief may gain access to this information. • The verbal disclosure of client personal information of an adult client to a family member of the client who is not the client’s authorized representative or legal guardian—this is successful unauthorized access and an improper disclosure. • An email containing CPI sent inside the state network but to wrong person in another agency—unauthorized access has occurred. • A virus or other malware is detected on a state computer (or a personal computer legitimately being used for state business)—at a minimum this is interference with system operations and, depending on the type of malware, may lead to unauthorized access to CPI. • A case worker shows a client personal information about the client on a computer screen, but discovers the information does not belong to that client (it was incorrectly attached to the wrong client file)—this is an improper disclosure resulting in unauthorized access to client personal information. • Unauthorized access to an application — this may lead to unauthorized access to CPI and is an intrusion; unauthorized access can occur from a variety of sources ranging from someone obtaining an authorized user’s ID and password to an external intrusion (hack) into the system. With respect to certain federal agency reporting of security incidents (e.g., SSA, IRS, CMS), the term security incident is further defined as: a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. This includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of
--	--

FSSA Privacy & Security Compliance Policies & Procedures

		mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction. While certain adverse events, (e.g., floods, fires, electrical outages, excessive heat, etc.) can cause system crashes, they are not considered incidents. An incident becomes a breach when there is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access to personally identifiable information (PII) or protected health information (PHI), whether physical or electronic. Reference the FSSA Privacy & Security Office Incident Notification Procedures for further discussion on Security Events and Security Incidents.
Privacy/Security Liaison		Reference Section 4 of these Privacy & Security Compliance Policies for an explanation. Also referred to as PSL.
Protected Health Information—PHI		Information that relates to an individual's past, present, or future physical or mental health or condition, including the provision of healthcare to the individual, <i>and</i> the past, present, or future payment for healthcare, and which identifies the individual (or which can be used to identify the individual). For example, a Medicaid claim is PHI; an individual's application for a disability waiver program is PHI. PHI is specifically protected by HIPAA.
Safekeeping		Client personal information that is created, obtained, maintained, and used by FSSA in its normal course of business, regardless of form, for which there is a reasonable expectation or regulatory requirement that the information is to be kept secure, confidential, and not improperly changed. This includes client personal information created, obtained, maintained, and/or used by a third party on FSSA's behalf (and under contract with FSSA for services that require use of client personal information). In particular, PHI and PII are to be safely kept.
Section 1176 of the Social Security Act		This section establishes the penalties for failure to comply with the provisions of the HIPAA Privacy Rule. The penalties are tiered based on the nature and circumstances of the offense and range from \$100 per violation (with an annual

		limit of \$25,000 for repeatedly violating the same provision) to \$50,000 per violation (with an annual limit of \$1.5 million for repeatedly violating the same provision). Sections 13401 and 13404 of HITECH provides that these penalties apply to Business Associates, as well as covered entities.
Section 1177 of the Social Security Act		This section establishes the penalties for person or covered entity who knowingly violates the HIPAA Privacy Rule: 1. Be fined not more than \$50,000, imprisoned not more than 1 year, or both; 2. If the violation is committed under false pretenses, be fined not more than \$100,000, imprisoned for not more than 5 years, or both; and 3. If the violation is committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both. Sections 13401 and 13404 of HITECH provides that these penalties apply to Business Associates, as well as covered entities. Section 13409 of HITECH clarified that these penalties also apply to individuals (including employees).
State Email		Means email used by FSSA personnel to conduct the state's business on behalf of FSSA and the State of Indiana—the content of the email, including attachments, is for state or FSSA business. Typically, this is email generated from or sent to your State Email Account. Contrasted with personal email used by staff to conduct their personal business; typically, this is email generated from or sent to your personal email account (like Gmail, Yahoo, Hotmail, Comcast, ATT, etc.).
State Email Account		Your State Email Account (or Address) is the fssa.in.gov email address assigned to you by FSSA Account Control/IOT. For example: John.Doe@fssa.in.gov <u>All FSSA email accounts end in fssa.in.gov.</u>
State Network		This is the technical infrastructure provided and managed by the Indiana Office of Technology (IOT) used for access to state systems (e.g., ICES) and email communications.

		With respect to email: “Inside the State Network” means that email from one fssa.in.gov email address is sent to or received from another fssa.in.gov email address. Whereas, “Outside the State Network” means the email is either sent to or received by a non-fssa.in.gov email address over the Internet. For example: John.Doe@fssa.in.gov to Jan.Doe@anthem.com. This email would be transmitted outside the state network as it is going to a company (non-state) email account over the Internet. This would include email from or to a staff member’s personal email account, whether or not the email is sent or received while you are at work. Alert: personal email is processed by the email host service (e.g., Google for gmail.com, Microsoft for Outlook.com, AT&T for att.net, etc.). This means your personal email goes through their computer systems and network and may or may not be secure. In addition, because these are Internet-based email services, your personal email could literally travel the world before it reaches its destination; this includes any fssa.in.gov email sent outside the state network (i.e., to a non-fssa.in.gov email address).
State Webmail		This term refers to access to State Email, Calendar, Contacts, and other IOT-provided services accessible from the Internet at https://outlook.office365.com.
Workforce Member		Means FSSA state employees, volunteers, interns, trainees, contractors, and other persons whose conduct, in the performance of work for FSSA, is under the direct control of FSSA, whether or not they are paid by FSSA. This includes contractors engaged by the IDOA Managed Service Provider. The terms <i>personnel</i> and <i>staff member</i> as used in FSSA policies and procedures both mean Workforce Member.

Section 17: Citations & Authorities

These FSSA Privacy & Security Compliance Policies and supporting procedures have been developed under certain federal and state laws and regulations, including but not limited to:

- 45 CFR Parts 160, 162 & 164, Health Insurance Reform: Security Standards; Final Rule (effective April 21, 2003)—HIPAA Security Rule
- 45 CFR Parts 160 & 164, Subpart E, Standards for Privacy of Individually Identifiable Health Information; Final Rule (as amended; effective April 14, 2003)—HIPAA Privacy Rule
- 45 CFR Parts 160 & 164, Subpart D, Breach Notification for Unsecured Protected Health Information; Interim Final Rule (effective September 23, 2009)—HIPAA Breach Notification Rule
- 45 CFR Parts 160 & 164, Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable (effective April 17, 2009)—HIPAA Encryption Guidance
- 45 CFR 155.260 Privacy and security of personally identifiable information
- 45 CFR 155.280 Oversight and monitoring of privacy and security requirements
- 42 CFR Part 431, Subpart F Safeguarding Information on Applicants and Recipients (Medicaid)
- 42 CFR Part 2 safeguards for mental health records
- 7 CFR 272.1(c) Use and disclosure restrictions for Food Stamps applicants/recipients
- 45 CFR 205.50 Safeguarding information for financial assistance programs (TANF)
- 34 CFR 361.38 Protection, use, and release of Personal Information (Vocational Rehabilitation)
- 34 CFR Part 99 (FERPA) privacy of educational records
- IDEA Parts B & C (First Steps); 34 CFR Parts 300 & 303 (confidentiality of student records)
- IC 12-15-27-1 Medicaid applicants and recipients; confidential records and documents
- IC 4-1-11, Notice of Security Breach (effective July 1, 2006)
- IC 4-1-10, Release of Social Security Number (effective July 1, 2006)
- IC 4-1-6, Fair Information Practices; Privacy of Personal Information (reference for dates)
- IC 12-14-1-7 Confidentiality of TANF records
- IC 5-14-3 Access to Public Records
- IC 16-36-1 Health Care Consent
- IC 16-39-2 Release of Mental Health Records
- IC 4-13.1 Office of Technology (authority to establish state security standards and policies)
- The Privacy Act of 1974, 5 U.S. Code § 552a
- IRS Publication 1075 (September 2016 Revision)
- Catalog of Minimum Acceptable Risk Controls for Exchanges (MARS-E)— Exchange Reference Architecture Supplement (Version 2.0, November 10, 2015)

In addition, the state's technology security standards and polices as defined in the IOT Security Framework and the IOT Tier 1 Security Standards (available to authorized personnel in the RSA Archer tool employed by IOT).

Section 18: Policy Administration

Updates and Version Control

Version	Revision Date	Revision Purpose	Completed By
1.0--Draft	July 27, 2012	Initial Release for Comment Period of 7/30/2012-8/30/2012	Cliff McCullough
1.0	November 27, 2012	Final version incorporating comments from the Comment Period	Cliff McCullough
2.0	August 27, 2014	Updated to include pertinent MARS-E requirements.	Cliff McCullough
3.0	May 21, 2018	Updated to include MARS-E 2.0 requirements and the IRS Background Check Policy	Cliff McCullough
4.0	December 20, 2019	Updated with minor revisions regarding State Webmail access and to address IRS and OCSE requirements.	Cliff McCullough
5.0	July 21, 2021	Updated with minor revisions and general language specifically regarding email encryption.	Jordan Lake and Cliff McCullough
6.0	December 30, 2022	Updated with minor revisions and general language specifically regarding faxing of FTI.	L. Scott Munoz and Cliff McCullough
7.0	January 31, 2024	Updated with minor revisions to address federal audit findings.	Cliff McCullough
8.0	January 3, 2025	Updated with AI and insider threat policies.	Cliff McCullough
9.0	January 2, 2026	Updated to include revisions to the FSSA FTI policies and clarification of the role based access policies.	Cliff McCullough

Annual Review

These FSSA Privacy & Security Compliance Policies and Procedures 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.

Signature Page

Related Policies: Replaces FSSA AD1-17 and FSSA AD1-18
Legal Reference: [Section 17: Citations & Authorities](#)
Originating Office: FSSA Privacy & Security Office
Effective Date: December 31, 2012

Approval: 
Michael A. Gargano, Secretary
Indiana Family & Social Services Administration

Effective Date: October 5, 2014

Authorized by:  on: 8/29/14
John J. Wernert, M.D., Secretary Date

Effective Date: July 15, 2018

Authorized by:  on: 5/23/18
Dr. Jennifer Walthall, Secretary Date

Effective Date: December 20, 2019

Authorized by:  on: 11/4/19
Dr. Jennifer Sullivan, Secretary Date

Effective Date: September 30, 2021


Authorized by: _____ on: 8/27/2021
Daniel Rusyniak, M.D., Secretary Date

FSSA Privacy & Security Compliance Policies & Procedures

Effective Date: December 30, 2022



Authorized by:

Daniel E. Rusyniak, M.D., Secretary

on: 11/4/2022

Date

Effective Date: January 31, 2024



Authorized by:

Daniel E. Rusyniak, M.D., Secretary

on: 11/27/2023

Date

Effective Date: January 3, 2025



Authorized by:

Daniel E. Rusyniak, M.D., Secretary

on: 10/30/24

Date

Effective Date: January 2, 2026



Authorized by:

E. Mitchell Roob Jr., Secretary

on: 11/14/2025

Date