



# **FSSA POLICY**

## **IDENTIFICATION AND AUTHENTICATION SECURITY POLICY**

EXECUTIVE POLICY #: 2014-010-IT

Effective Date: **October 5, 2014**

### **Revision History**

Version 1.0 – July 01, 2014: Initial policy created for comment period.

Version 1.1 – August 28, 2014: revisions applied

### **Purpose**

The purpose of this policy is to establish identification and authentication measures and procedures to manage the risk associated with user access and authentication activities. Implementation of strong identification and authorization mechanisms will decrease the risk of unauthorized users gaining access to FSSA information systems. The policy statements below contribute to the FSSA information security program by enumerating the best practices with regard to identification and authentication policy and associated identification and authentication controls. This policy serves to supplement Indiana Office of Technology, Indiana Code and any applicable federal compliance statutes.

### **Scope**

This policy applies to information systems in use at FSSA.

### **Definitions**

#### **Application**

An application is composed of one or more pieces of computer programs. Applications may perform functions in an automated fashion using clearly defined rules to facilitate business goals and meet objectives. Applications require special consideration due to the sensitivity of the information they create, manipulate, maintain, or transmit.

#### **Authentication**

Authentication is the process of verifying the claimed identity of a user. Authentication information should be kept confidential. Authentication is often discussed in terms of the three factors of authentication: something that is known to the individual; something that the individual has; and something that the individual is.

### **External information systems**

External information systems are information systems which the FSSA or IOT has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. An external information system may be an Internet kiosk, personally owned phone or tablet device, or public computer in a hotel, library or airport.

### **Identification**

Identification is the process whereby a network element recognizes a valid user's identity. A user may be a person, a process, or a system (e.g., an operations system or another network element) that accesses a network element to perform tasks or process a call. Information used to verify the claimed identity of a user can be based on a password, Personal Identification Number (PIN), smart card, biometrics, token, exchange of keys, etc.

### **Identifier**

An identifier is a name, label, code or symbol that labels the identity of an individual, device or object.

### **Information systems**

Information systems are identified by constructing logical boundaries around a set of processes, communications, assets, applications, storage locations and related components. These components collect, store, and process data. FSSA information systems are used to help the agency effectively and efficiently deliver human and social services.

### **Internal networks**

Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the State of Indiana.

### **IRS Publication 1075**

Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (PDF) contains specific requirements for safeguarding federal tax information.

### **Local access**

Local access is any access to an information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network.

### **MARS-E**

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

### **Network access**

Network access is any access to an information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection.

### **Privileged system user**

An individual that is responsible for complying with all security requirements in order to obtain access to an information system. Privileged users (e.g. root or administrator) have a unique role

within an organization as they are granted rights within the computer system which are significantly greater than those available to the basic system users.

### **Protected information**

Protected information is a catch-all phrase for certain types of data, material, and facts that are linked to an individual which are protected under state or federal law. Information protected by Health Insurance Portability and Accountability Act of 1996 [Public Law 104-191] (HIPAA) is called Protected Health Information (PHI). Information protected under IC 4-1-6 or IC 4-1-11 is called Personally Identifiable Information (PI/PII). Federal Tax Information (FTI) is any tax return-derived information received from the Internal Revenue Service. Identifiable client data is referred to as client personal information (CPI) in the FSSA Privacy & Security Compliance Policies manual.

### **Remote access**

Remote access is a type of network access which allows an organization's users to access its nonpublic computing resources from locations other than the organization's facilities and often involves communication through an external network (e.g., the Internet).

### **Security controls**

Security controls are safeguards or countermeasures intended to offset or minimize security risks. The security control guidance is selected from "The Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement". The MARS-E is based on NIST SP 800-53 with additional controls of IRS Publication 1075 to address the handling of IRS Federal Tax Information (FTI). The controls for the most part share significant similarity to the NIST 800-53.

### **System owner**

The system owner is defined as an individual or group of individuals with responsibility for having the information system operated and maintained. System owners coordinate and oversee the successful execution of sound operating practices thereby insuring compliance to established security policies. System owners obligate their service provider or vendor providing service to adhere to legal and regulatory requirements regarding applicable programming, database, and hardware standards. Information system administrators, analysts, developers, engineers, or consultants are obligated to operate, implement, and/or manage an information system on behalf of a system owner in a manner that ensures the confidentiality, integrity and availability of FSSA client data.

### **User account**

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

## **References**

Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement - <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Catalog-of-MinAcceptable-Risk-Controls-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>

FSSA Privacy & Security Compliance Policies - [http://intranet.fssa.in.gov/SiteCollectionDocuments/LinkedFiles/HIPAA/FSSA\\_Privacy\\_Compliance\\_Policies.pdf](http://intranet.fssa.in.gov/SiteCollectionDocuments/LinkedFiles/HIPAA/FSSA_Privacy_Compliance_Policies.pdf)

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

IOT Information Security Framework - [http://intranet.iot.in.gov/security/SharedDocuments/Practice 8.2.1 - End User Password Minimums.pdf](http://intranet.iot.in.gov/security/SharedDocuments/Practice%208.2.1%20-%20End%20User%20Password%20Minimums.pdf)

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

IOT Two Factor Authentication Practice - [http://intranet.iot.in.gov/security/SharedDocuments/Practice 8.4.1 - 2 factor authentication.pdf](http://intranet.iot.in.gov/security/SharedDocuments/Practice%208.4.1%20-%202%20factor%20authentication.pdf)

NIST Special Publication 800-53 (Rev. 4) Control - Security and Privacy Controls for Federal Information Systems and Organizations - <http://web.nvd.nist.gov/view/800-53/Rev4/>

NIST Special Publication 800-114 - User's Guide to Securing External Devices for Telework and Remote Access - <http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf>

## **Policy Statement(s)**

FSSA identification and authentication policy standards establish effective implementation of security controls and control enhancements in the NIST and CMS MARS-E identification and authentication control family.

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

1. FSSA shall have an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance which shall be reviewed and updated as necessary every three-hundred-sixty-five (365) days [IA-1].
2. FSSA users must uniquely identify and authenticate into information systems. Authentication of user identities shall be accomplished through the use of strong passwords, tokens, biometrics, multi-factor authentication, or some combination thereof. In addition to identifying and authenticating users at the information system level (i.e., at logon) identification and authentication mechanisms shall be employed at the application level, when necessary, to provide increased information security for the organization [IA-2].
3. For FSSA information systems impacted by CMS MARS-E requirements information systems must use multifactor authentication for local access to privileged accounts [IA-2(3)].
4. Identifiers for users and devices must be unique and assigned to the intended object. FSSA authentication and identification standards prohibit reuse of user or device identifiers for the period to which an identifier is assigned to an active user or device. A device or user identifier shall not be reused until all previous access authorizations are removed from the information system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired [IA-4].
5. FSSA shall insure that information systems which utilize password-based authentication as a single factor to authenticate users must [IA-5, IA-5(1)]:
  - a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
  - b. Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days;
  - c. Prohibits the use of dictionary names or words;
  - d. Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters;
  - e. Enforces at least a minimum of four (4) changed characters when new passwords are created;
  - f. Encrypts passwords in storage and in transmission;
  - g. Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum;

- h. Prohibits password reuse for six (6) generations prior to reuse.
- i. Protecting authenticator content from unauthorized disclosure and modification

7. For information systems that are in scope of IRS Publication 1075 safeguards and utilize password-based authentication as a single factor to authenticate users, those systems must change/refresh authenticators every 90 days, at a minimum, for a standard user account, every 60 days, at a minimum, for privileged users [IA-5(1)].

8. FSSA information systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or misuse by unauthorized individuals [IA-6].

**Exemption(s):**


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

**Enforcement:**

Noncompliance with this policy and stated implementation standards may result in loss of data access privileges, systems being taken offline, or personnel sanctions in accordance with state and FSSA policy.

**Roles and Responsibilities:**

FSSA is responsible for adhering to the security standards, procedures or guidelines referenced by the above policy.

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