Michael R. Pence, Governor
State of Indiana

Indiana Family and Social Services Administration

FSSA POLICY

ACCESS CONTROL POLICY

EXECUTIVE POLICY #: 2014-004-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 access control measures and procedures. Controlling access to information systems is critical to ensuring the confidentiality, integrity and availability of FSSA client data. The policy statements below contribute to the FSSA information security program. An effective information security program improves FSSA's security posture and aligns information security with FSSA's mission, goals, and objectives. This policy serves to supplement Indiana Office of Technology, Indiana Code and any applicable federal compliance statutes.

Scope

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

Definitions

Anonymous account

An anonymous account is equal to a public or guest user which has no known affiliation with the agency or identifiable distinction.

Authorization

A formal administrative approval required for an individual to gain access to a facility, system, or other information asset is known as authorization.

Access Control(s)

The rules and deployment mechanisms which control physical and logical access to information systems are known as access controls. Access controls protect things perceived to be of value.

Basic System User

An individual that is responsible for complying with all security requirements in order to obtain fundamental and primary access to an information system.

Emergency account
An emergency account is short term account that exists temporarily for a period of less than twenty-four (24) hours.

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

Information asset
An information asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and data. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the agency.

Information 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.

Least privilege
Assigning a user account only the most minimal rights required to access only the information and resources that are necessary to that user's work.

Logical Access Controls
Logical access controls are most often associated with login credentials procedures that grant or deny individuals the ability to read, write, or execute records or data contained in the information system.

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

Physical Access Controls
The ability to access areas or premises where information systems and technology assets reside depends on physical access controls. Physical access controls can be as basic as a locked door or as sophisticated as anti-pass-back mechanisms and man trap areas.

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.

RBAC
Role-based access control provides a level of abstraction to establish permissions based on functional roles. Access decisions to systems and data are based on the role a user may have in the organization or information system. Roles may represent a task, position, responsibility or function assumed by an individual in a system.

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.

Temporary account
A temporary account is an account that provides access for a limited duration to a system. Such an account may be granted to a user who may not have a long term affiliation with an agency. These accounts are often intended to expire within three-hundred-sixty-five (365) days.

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 - https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Catalog-of-MinAcceptable-Risk-Controls-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf

FSSA Privacy & Security Compliance Policies - http://intranet.fssa.in.gov/SiteCollectionDocuments/LinkedFiles/HIPAA/FSSA_Privacy_Compliance_Policies.pdf

IOT Information Security Framework - http://in.gov/iot/2339.htm

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

Policy Statement(s)

The FSSA access control security standards define the physical and logical access control measures that appropriately limit access to FSSA information, processing systems and facilities to authorized individuals except where designated for public access.

FSSA Access Control Standards

1. FSSA shall have documented procedures and/or guides and handbooks to facilitate the implementation of the access control policy and associated access controls which shall be reviewed and updated as necessary every three-hundred-sixty-five (365) days. These documents must define and map individuals into specific user roles that enforce least privilege. Roles are to be based on business needs and security requirements. Procedures, guides or handbooks must define the authorization process for granting access to FSSA information resources [AC-1].

2. FSSA shall review user accounts every one-hundred-eighty (180) days to modify, disable, or remove that are invalid, inactive, no longer required or no longer meet the attributes required for the mission or business function [AC-2]. Automated mechanisms to support the management of information system accounts should be employed where possible [AC-2(1)]. User accounts must identify a unique individual or device. User accounts shall not be reused or reassigned before a period of at least three hundred sixty-fixe (365) days has passed [IA-4].

3. If any FSSA information system should utilize an emergency or temporary account then the account itself must be monitored and tracked after it is authorized for use by the system owner (or designate). System owners must be notified when temporary accounts are no longer required. Emergency accounts must terminate automatically within twenty-four (24) hours. Temporary accounts must not be in existence for more than three-hundred-sixty-five (365) days [AC-2(2)].

4. FSSA shall ensure that each user is assigned a role that is commensurate with their job duties [AC-5, AC-6]. Roles must ensure the maximum possible security for systems and data while providing flexibility for configuration and management. Role assignments must be formally tracked and monitored; in particular FSSA must inspect administrator groups, root accounts and system accounts at least once every fourteen (14) days [AC-2(7), AC-6(2)] for accuracy.

5. FSSA systems must protect individual authenticators (ex: passwords, tokens) [IA-5(1)] from unauthorized disclosure and modification. If encryption is employed for FSSA systems in scope of the CMS MARS-E or IRS Publication 1075 requirements then the cryptographic modules must comply with applicable federal standards, guidance and enhancements [SC-8, SC-9, and SC-17].

6. FSSA shall ensure that the flow of information between sources and destinations within and between information systems is documented and authorized. The confidentiality and integrity [SC-8] of data must be maintained as information traverses multiple systems and boundaries [AC-4]. Security controls such as firewalls, security appliances, filtering and network segmentation facilitate the separation and flow control of data.

7. FSSA shall place limits on consecutive invalid login attempts during a specified time period [AC-7]. Concurrent sessions for each system account must be limited to the number of sessions expressly required for the performance of job duties. Any requirement for more than one (1) concurrent application/process session shall be documented in the respective system's security plan [AC-10]. In addition information systems shall require a user to reestablish access using established authentication and identification procedures after fifteen (15) minutes of inactivity. Any requirement for a longer duration session shall be documented in the respective system's security plan [AC-11].

8. Remote access to FSSA systems for the purpose of administration or execution of privileged commands shall be for compelling operational needs. Multifactor authentication [IA-2(1)] should be utilized for privileged users who access FSSA information systems remotely. The execution of remote access must be audited, documented and approved. Cryptography of sufficient strength [AC-17(2)] must be implemented to protect the confidentiality and integrity of remote sessions [AC-17(4)].

9. Only FSSA approved systems may be used to process, access, and store FTI, PHI, or PII; private, personal, or non-business information systems shall not be authorized for FTI, PHI, or PII [AC-20]. External information systems may not be utilized to create, manipulate, maintain, or transmit protected information. FSSA approved portable storage devices (approved encrypted USB drives and external hard drives) should not be utilized on external information systems [AC-20(2)] unless they are subject to the restrictions and conditions specified in the FSSA Privacy Compliance Policies & Procedures Section 7.

10. FSSA must ensure that publicly accessible information does not contain nonpublic information. Only FSSA designated individuals may post information onto an organization information system that is publically accessible. FSSA must remove nonpublic information from publicly accessible organizational information systems if discovered [AC-22].

Exemption(s):

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

Enforcement:

The FSSA access control security standards must be enforced. Assessment and validation procedures shall ensure access to information and assets is limited to only authorized persons except where designated for public access. 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