



FSSA POLICY

CONFIGURATION MANAGEMENT POLICY

EXECUTIVE POLICY #: 2014-007-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 configuration management control measures and procedures. Managing the risk introduced when changing information system configuration settings is critical to ensuring the confidentiality, integrity and availability of FSSA client data.

The policy statements below contribute to the FSSA information security program by enumerating the standards and procedures utilized to document, authorize, manage and control system changes. This policy serves to supplement Indiana Office of Technology, Indiana Code and any applicable federal compliance statutes.

Scope

This policy applies to all FSSA information systems.

Definitions

Baseline Configuration

A baseline configuration is a documented, up-to-date specification to which the information system is built. It provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

Configurable devices

Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

Configuration settings

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system.

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.

Information system and component inventory

Characteristics of an acceptable inventory of information system components are: accurate with respect to current configuration; sufficiently granular for tracking and reporting purposes; consistent with the authorization boundary of the system; enumerates manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.

MARS-E

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

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.

Secure configuration

Recognized, standardized, and established benchmarks that stipulate secure configuration settings are developed by a variety of organizations including manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. These secure configuration settings are applied to information assets by following specific instructions pertinent to the respective information technology platform and product. Once the settings are applied and validated, the asset may be considered to be in a secure configuration.

Security controls

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

Security functions

Security functions such as authenticating, auditing, encrypting, and authorizing are deployed in hardware, software or firmware.

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.

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>

IRS Publication 1075 Safeguards for Protecting Federal Tax Returns -

<http://www.irs.gov/pub/irs-pdf/p1075.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 800-128 Guide to Security-Focused Configuration Management of Information Systems - <http://csrc.nist.gov/publications/PubsSPs.html#800-128>

Policy Statement(s)

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

FSSA Configuration Management Standards

1. FSSA shall review and update as necessary within three-hundred-sixty-five (365) days the formal, documented configuration management policy [CM-1].
2. FSSA shall insure that a fully developed, accurate and complete [CM-8] inventory of its information systems and components is maintained [PM-5]. Inventory records must be updated during installations, removals, and updates [CM-8(1)]. A complete master information system inventory eliminates duplicate and inaccurate records in other collections thereby allowing for consistent and accurate baseline configurations to be developed and maintained [CM-8(5)].
3. A baseline configuration must be developed, documented, and maintained for FSSA information systems. FSSA information system baselines shall establish a common point of reference which are then reviewed and updated based on deviations from the baseline configuration in support of mission needs/objectives [CM-2].
4. Review of baselines shall occur at least once every three-hundred-sixty-five (365) days or after major information system changes such as new component installations or software upgrades or operating system upgrades [CM-2(1)].
5. FSSA information systems shall follow a formal process to ensure that changes to a system are introduced in a controlled and coordinated manner [CM-3]. FSSA shall record, assess, plan, test [CM-3(2)], and implement configuration-controlled changes to systems with explicit consideration for security impact [CM-4].
6. Records of configuration-controlled changes to FSSA information systems shall be maintained and periodically audited. Configuration-controlled changes to FSSA information systems must be coordinated and communicated appropriately. If changes such as upgrades or modifications are applied to FSSA information systems the security functions must be verified [CM-4(2)] to insure they continue to operate as intended. Detection of unauthorized, security-relevant configuration changes [CM-6(3), SI-7(1)] must be accounted for in the incident response function; detected events must be tracked, monitored, corrected, and available for historical purposes.
7. For FSSA information systems, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications [CM-5].

8. FSSA information systems must provide only essential capabilities. System services, ports, network protocols, and capabilities not explicitly required for system or application functionality must be disabled or restricted [CM-7]. Within every three-hundred-sixty-five (365) days FSSA information systems must be reviewed to identify and eliminate these unnecessary functions, ports, protocols, and/or services [CM-7(1)].

Exemption(s):

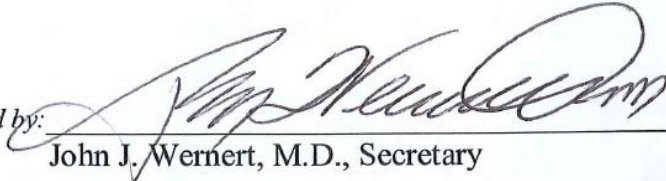
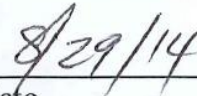
The FSSA Privacy & Security Officer along with the system owner shall determine if baseline exceptions or baseline exemptions for individual components configuration settings within the information system are acceptable [CM-6] based on consideration of the risk.

Enforcement:

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

Roles and Responsibilities:

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

Authorized by:  on: 
John J. Wernert, M.D., Secretary Date