Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

065.016 Configuration Management Policy

Version 2.6
July 27, 2021

Revision History

Date	Version	Description	Author
12/16/2011	1.0	Effective Date	CHFS IT Policies Team Charter
7/27/2021	2.6	Review Date	CHFS OATS Policy Charter Team
7/27/2021	2.6	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive Director (or designee)	7/27/2021	Jennifer Harp	DocuSigned by: Jennifer Harp 057B913AA3E14AE...
CHFS Chief Information Security Officer (or designee)	7/27/2021	Nicholas Tomlin	DocuSigned by: 55B6A12812DD403...

Table of Contents

1 Policy Definitions

- **Agency:** Defined by CHFS for the purpose of this document, agency or agencies refers to any department under CHFS.
- **Baseline Configuration:** Defined by National Institute of Standards and Technology (NIST) 800-53 Revision 4 as a documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law (Kentucky Revised Statute 61.878); Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e., System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Protected Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Identifiable protected health information items include many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- **Enterprise:** Defined by NIST 800-53 Revision 4 as an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, information systems, information and mission management.
- **Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable

information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61.931-934 and in accordance with NIST 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account; social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA). In addition, HIPAA identifies an individual's full name, date of birth, street or email address, biometric data, and other common identifiers as direct PII, not requiring a combined additional field of information.
- **Sensitive Data:** Defined by COT standards as data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: all information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information. The Commonwealth's proprietary information including but not limited to intellectual property, financial data and more.
- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS with final approval and appointment by the Kentucky Personnel Cabinet.
- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Application Technology Services (OATS) must establish a comprehensive level of security controls through a configuration management policy. This document establishes the agency's Application Configuration Management Policy to manage risks and provide guidelines for security best practices regarding configuration management.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within CMS, the IRS, and SSA.

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

An individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach. This position is responsible for adherence to this policy.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for the protection of the PCI, PII, ePHI, FTI and other financially sensitive information to all CHFS staff/personnel. This role, along with the CHFS OATS IS Team, is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas for providing full recovery of all application functionality as well as meeting federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 Baseline Configuration

CHFS agencies follow the Commonwealth Office of Technology (COT) OIS-053 Windows and ESX Baseline Configuration Documentation Annual Review Procedure (Note: Access to the above information requires special permissions, if more information is needed contact COT). This finalized process establishes the baseline security configuration for all Windows systems supported by the COT Windows Server Support Team.

CHFS follows Enterprise OIS-051 Security Configuration Documentation Annual Review Procedure (Note: Access to the above information requires special permissions, if more information is needed contact COT.) by reviewing baselines and updates for desktop, laptop, and printer components annually and during critical system patches, emergency patches, and/or major system updates, as required. COT is responsible for retaining older versions of baseline configurations for CHFS agencies servers, laptops, desktops, printers, network switches, and firewall components. CHFS agencies will retain configurations, current and past versions, for software components.

4.2 Configuration Change Control

CHFS agencies follow the CHFS 010.103- Change Control Policy and CHFS 065.014- CHFS SDLC and New Application Development Policy regarding change control guidelines. CHFS agencies and/or the enterprise will retain records of configuration-controlled changes to the Information System for a minimum of three (3) years.

4.3 Access Restrictions for Change

To ensure the completion of software application update reviews and implementation, the following policies/procedure are followed by CHFS agencies to document significant changes to software, hardware, communication links, and operational procedures:

- Enterprise Policy CIO-101 Enterprise Release Management Policy
- Enterprise Procedure: COT-067- Enterprise Security Standard Process and Procedures Manual (ESSPPM) Section 5.7.6- Hardware Changes/Configuration Management
- Enterprise Procedure: COT-009 Change Management

(Note: Access to the above information requires special permissions, if more information is needed contact COT point of contact.)

4.4 Configuration Settings

CHFS agencies will follow COT security configuration guidelines, which include mandatory baseline configuration settings for information systems. Any exceptions from these mandatory configurations must go through the formal CHFS approval process by following CHFS 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy, or the formal COT Security Exemption Request, COT-

F085 form process. Please note: Must be connected to the state network in order to access the forms.

4.5 Least Functionality

CHFS agencies are required to configure roles granting system access based on the principle of least privilege. COT prohibits and disables the use of high-risk system services, ports, network protocols, and capabilities across network boundaries that are not explicitly required for system or application functionality. COT supports the entire Commonwealth infrastructure for the agencies.

COT performs monthly vulnerability scans of networks, servers, and databases to identify unnecessary functions, ports, protocols and/or services. Based on the scanning results, COT coordinates with necessary agency personnel to remediate/disable unnecessary functions, ports, protocols, and/or services identified.

4.6 Information System Component Inventory

COT shall utilize the Procurement, Payables, and Asset Tracking System (PPATS) and Information Technology Management Portal (ITMP) for tracking IT hardware assets through their lifecycle from procurement to disposal. In addition to the PPATS and Information Technology Management Portal, the COT Asset Management Division maintains a current inventory of software under its control for quality assurance.

4.7 Configuration Management Plan

OATS Information Security (IS) Team recommends that each agency develop, document, and implement a configuration management plan for the information system. This plan shall include, but is not limited to the following:

- Addressing roles, responsibilities, configuration management processes, and procedures;
- Establishing a process for identifying configuration items throughout the System (Software) Development Life Cycle (SDLC) and managing the configuration of items;
- Defining configuration items for information systems and place the configuration items under configuration management; and
- Protecting the configuration management plan from unauthorized disclosure and modification.

National Institute of Standards and Technology (NIST) Special Publication 800-128 Revision 1, Guide for Security-Focused Configuration Management of Information Systems- Appendix D can be referenced and used as a guide/sample for agencies when creating a configuration management plan.

4.8 Software Usage Restrictions and User Installed Software

The COT Division of Asset Management is responsible for periodically reviewing compliance of software licenses and copyright policies. Additionally, each COT department's management is responsible for ensuring that the necessary

documentation is available to provide proof of proper software acquisition. COT-067: ESSPPM, Section 3- Logical Security Processes and Procedures ensures standardized configurations for hardware and software. For security reasons, the installations of unauthorized applications are not permitted on the network. Any unauthorized applications will be removed and the user may be subject to disciplinary actions.

Any exceptions from these mandatory configurations must go through the formal CHFS approval process by following the Enterprise Kentucky Information Technology Standards (KITS) Exception Request Form, COT-027, or the formal COT exception process following Security Exemption Request, COT-F085.

5 Policy Maintenance Responsibility

The CHFS OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as-needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 010.103- Change Control Policy
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS Procurement, Payables, and Assets Tracking System (PPATS)
- Enterprise IT Policy: CIO-101- Enterprise Release Management Policy
- Enterprise IT Procedure: COT-067: Enterprise Security Standard Process and Procedures Manual (ESSPPM)
- Enterprise Security Exemption Request, COT-F085
- Enterprise Kentucky Information Technology Standards (KITS) Exception Request Form, COT-027
- Information Technology Management Portal (ITMP)
- Internal Revenue Services (IRS) Publication 1075

- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-128 Revision 1, Guide for Security-Focused Configuration Management of Information Systems
- Social Security Administration (SSA) Security Information