Commonwealth of Kentucky
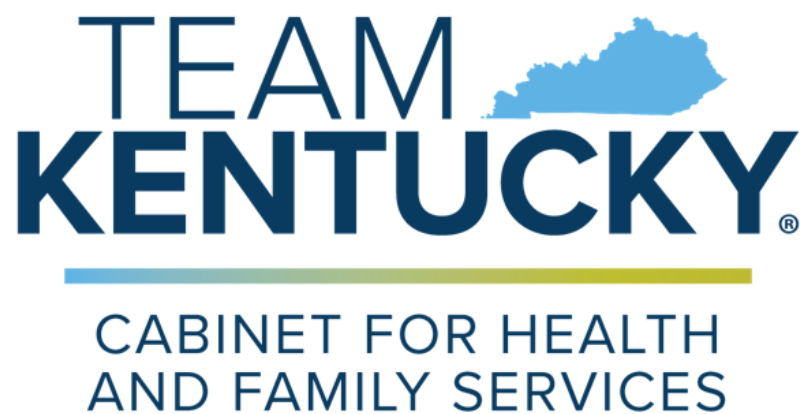Cabinet for Health and Family Services

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

065.021 Kentucky Online Gateway (KOG)
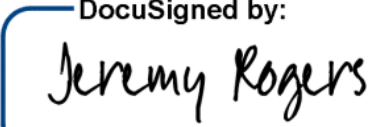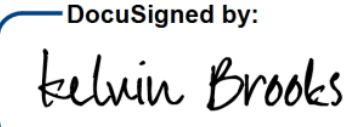**Application Configuration Management Policy**

Version 1.6
August 7, 2024

Revision History

Date	Version	Description	Author
10/5/2018	1.0	Effective Date	CHFS Policy Charter Team
08/07/2024	1.6	Review Date	CHFS Policy Charter Team
08/07/2024	1.6	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive Director (or designee)	8/7/2024	Jeremy Rogers	DocuSigned by: Jeremy Rogers FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or designee)	8/5/2024	Kelvin Brooks	DocuSigned by: Kelvin Brooks A0F3F24DC182406...

Table of Contents

1 Policy Definitions

- **Access:** Defined by CHFS as the ability to use or modify an information resource.
- **Application:** Defined by CHFS as a software program designed to perform a specific function (e.g., Partner Portal, Benefind, etc.).
- **Business Partner:** Defined by CHFS as the agency in which the system/data owner has granted permission for use of a designated application.
- **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.
- **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 National Institute of Standards and Technology (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.
- **System/Data Administrator:** Defined by CHFS as an individual who is responsible for the data administration process by which data is monitored, maintained, and managed. This person is responsible for controlling application data assets, as well as their processing and interactions with different applications and business processes. This person is also tasked with access management to the system/data using the Role-based Access Control (R-BAC) model. In the Cabinet for Health and Family Services, this role is generally assigned to a CHFS Branch Manager.
- **System/Data Custodian:** Defined by CHFS as an individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department, which owns the Infrastructure. The duties include performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the enterprise security policies, standards, and guidelines that pertain to information security and data protection. In the Commonwealth of Kentucky, this role is generally assigned to the Commonwealth Office of Technology (COT).
- **System/Data Owner:** Defined by CHFS as the person who has final agency responsibility of data protection and is the person held liable for any negligence

when it comes to protecting the specific application's data/information assets. This role/person is the owner of the system that holds the data. Typically, a senior executive designates the confidentiality of the system/data, and assigns the data admin, and dictates how the information should be protected based on business' policies. In the Cabinet for Health and Family Services, this role is generally assigned to a CHFS Business Executive.

- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through a formal contract such as the System Design/Development Services (SDS) contract or other approved agreement, to provide temporary work for CHFS.
- **Worker Type:** Defined by the Enterprise Kentucky Online Gateway (KOG) as the logical containers in which workers are grouped, based on the application access required and the type of work that they perform in order to fulfill their job responsibilities.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive level of security controls through configuration management guidelines. This document establishes the agency's Application Configuration Management Policy, which helps manage risks and provides guidelines for privacy and security best practices regarding the configuration of applications housed in the Kentucky Online Gateway (KOG).

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

Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Advisor 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

Coordination within organizations and/or agencies with the cabinet, which 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. Applicable agencies additionally 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 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 Chief/ Deputy Chief Technology Officer (CTO)

This individual makes decisions related to a company's technology. This includes the integration and deployment of new technology, systems management and the overseeing of technical operations personnel. The CTO also works with outside vendors to ensure they meet customer service expectations. This individual is responsible for adherence to this document.

3.4 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 PCI, PII, ePHI, FTI and other sensitive information to all CHFS staff/personnel. This role, along with the CHFS IS Team, is responsible for adherence to this policy.

3.5 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 information system(s).

3.6 System Data Owner and System Data Administrators

Management/lead who work with the application's development team to document components that are not included in the base server build and ensure functionality and backups are conducted in line with business needs. This individual(s) will be responsible to work with enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 General

The purpose of this policy is to ensure that all application configuration requests and updates are reviewed and implemented in a rational and predictable manner. Effective application and enforcement of these standards are essential to ensure reliable delivery of services.

Application owners are responsible for the following when requesting new application configurations, role configurations, and URL configurations, and/or changes to current configurations within KOG:

1. The application owners will send request to the KOGConfigurationManagement@ky.gov inbox so the team can send the application owner the Application Configuration Form.
2. Application owners need to fill out the Application Configuration Form and send it back to the KOG team at least forty-eight (48) hours prior to the requested deployment date.
3. A list of business partners responsible for submitting provisioning access request for users
4. An approval workflow and/or credential workflow process for an access request, including named workflow approvers.
5. Requirement for initial access for users, either through bulk load or individual access request, by designated business partners

Once the new application configuration has been completed by the KOG Technical Team, training will be provided by the KOG Business Team to the application owner(s) if required. The configuration will then be assigned to the KOG Technical Team for configuration of the Relying Party Trust in Active Directory Federation Services (ADFS) and the provisioning of user accounts. Upon completion of the application configuration by the KOG Technical Team, a notification will be sent to the application owner for provisioning staff.

Once the initial provisioning has been completed, additional access requests to the application must be granted as follows:
- If provisioning was completed through a bulk load, any additional users must be added through the Access Request process initiated by the Business Partners, which can be found in the online KOG Request Application.
- Provisioning of additional worker types will be granted through the Application Owner via email to KOGConfigurationManagement@ky.gov.

When application access is granted by submitting an Access Request through KOG, the action goes through an approval workflow process before the application can be

accessed by the end user through KOG. The approval workflow contains named individuals responsible for approving employee access within the organizational structure; therefore, it is the responsibility of the application owner and/or designated business partners to notify the KOG team of staffing changes resulting in additions and deletions to the workflow. Failure to notify the KOG team of these staffing changes can result in a delay and/or denial of workflow requests submitted through the KOG request application. Updates to the workflow can be submitted via email to KOGConfigurationManagement@ky.gov. All email requests will be retained for a period of five (5) years from the date of the request.

When an application or role within an application is no longer utilized, the application owner will be required to send the request to remove the application or role from the existing worker type templates. This request is to be submitted via email to KOGConfigurationManagement@ky.gov. All requests submitted to KOG will be completed within forty-eight (48) business hours.

5 Policy Maintenance Responsibility
The 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 Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Controls 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 2.2
- CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Controls Policy
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Online Gateway (KOG)
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information