Commonwealth of Kentucky
Cabinet for Health and Family Services

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

020.301 CHFS Network-User Account Policy

Version 2.6
February 4, 2021

Revision History

Date	Version	Description	Author
9/2/2002	1.0	Effective Date	CHFS OATS Policy Charter Team
02/4/2021	2.6	Review Date	CHFS OATS Policy Charter Team
02/4/2021	2.6	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	02/4/2021	Jennifer Harp	DocuSigned by: Jennifer Harp 057B913AA3E14AE...
CHFS Chief Information Security Officer (or designee)	01/28/2021	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 within CHFS.
- **Application Source Code:** Human-readable text written in a specific programming language.
- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation not to 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; 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 Personal 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 Identity Management (EIM):** Defined by the Enterprise Identity Management User Guide as the Commonwealth Office of Technology's (COT) solution for identity management for employees and other users in the Commonwealth. EIM is a centralized system designed to standardize account creation, modification, and removal for users in the Commonwealth. EIM manages Active Directory, Email, and Home Folder(s).
- **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.

- **Network Access:** Defined by CHFS as access to servers, Active Directory, databases, folders, within or on the CHFS boundaries.
- **Obfuscated Data:** Defined by the National Institute of Standards and Technology (NIST) 800-122 as data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated.
- **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.
- **Production (PROD):** Defined by CHFS as the system environment where the intended users will interact with the system and is updated only when testing on other environments is completed. Data within the system environment that may contain personal, identifiable, sensitive, and confidential information. All servers shall be labeled in the Information Technology Management Portal (ITMP) to reflect the system environment (i.e. Development, Test, Production, etc.).

  Production data is prohibited to be accessed by any contract, state, vendor, or other personnel located offshore. All users requesting production data must be located within the United States. This applies to all CHFS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. By definition, production data is classified as "production data" when located in any environment. If production data is obfuscated, it is then not considered live production data, as such, obfuscated data may be accessed via offshore personnel.
- **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 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 network-user account policy. This document establishes the agency's Network-User Account Policy, to help manage risks and provide guidelines for security best practices regarding network accounts and access.

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 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 NIST. Applicable agencies additionally follow security and privacy frameworks outlined within CMS, IRS, and SSA.

3 Policy 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 protection of Payment Card Industry (PCI), PII, ePHI, FTI and other sensitive information to all CHFS staff and contract personnel. This role along with the CHFS OATS IS Team is responsible for adhering 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 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.

3.6 Kentucky Online Gateway (KOG) Enterprise Identity Management (EIM) Administrators

Authorized KOG personnel are responsible for taking electronically submitted service requests received by KOG and submitting them to the Commonwealth Service Desk (CSD) for completion. These authorized staff personnel are responsible for basic validation of service request information and are listed as an approved IT service contact to submit service desk tickets for CHFS. Questions regarding KOG EIM Administration can be submitted to the CHFSServiceRequests@ky.gov mailbox.

3.7 Service Requestor

CHFS Division Directors are approved designated individual(s) having access to submit requests for users to obtain database, server, local admin, and RSA hard token access. The requestor shall submit appropriate forms (as listed in the Procedure below) to the designated secure SharePoint Access Tracker. Approved/Appointed OATS Service Requestors can be found within the Approved OATS Service Requestors List.

4 Policy Requirements

4.1 General Information

CHFS adheres to Commonwealth Office of Technology (COT) Enterprise Policy: CIO-072- Identity and Access Management Policy. Maintenance of CHFS Domain accounts is coordinated through COT.

The immediate supervisor of a new employee is responsible for ensuring the employee reads and agrees with all information provided through the Office of Human Resource Management (OHRM) Personnel Handbook. CHFS employees must read, understand, and sign the CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219) upon initial hire and annually thereafter. The immediate supervisor, or designee, is responsible for requesting the creation, modification, or deletion of an employee's CHFS Domain account, as needed, through the Kentucky Online Gateway (KOG).

CHFS staff must coordinate with the KOG team to obtain mainframe user access. Through the KOG Request application, the designated requestor for the user's department shall submit a request for mainframe access and must obtain a completed CHFS-219B form from the user prior to gaining access to the mainframe.

4.2 Domain Account Creation

Newly hired/on boarded state staff are entered into the Human Resource (HR) KHRIS system. Once actions are approved and completed in KHRIS, employee data is automatically sent to EIM, and the domain account is created. This information is then synced to KOG.

Newly hired/on boarded contract/vendor staff work with the agency/division's service requestor for a request to create a domain account through KOG. Once KOG receives the request, KOG Administrators manually retain and input the data into EIM. Once KOG Administrators complete the process, the contract/vendor staff's domain account is created.

4.3 Application Access

Contract, state, and vendor staff requesting application access, work with the agency/division's service requestor to submit a request via KOG. The KOG's Request

Application Portal is utilized by the Service Requestor for requesting user access. The request is then routed through an automated workflow for approval.

4.4 Network Access

After a state or contract/vendor's account is created, and if deemed necessary, access to network resources (i.e. database, server, etc.) may be requested by appropriate management. The following COT forms must be filled out when the user is requesting production and/or UAT access:

- F181- Staff Service Request Form
- F085- Security Exemption Form

*Note: If Development or Test access is requested, an F085 is not required unless access is being requested for a vendor. For vendor access the F085 is required for all environments.

4.5 Removal/Deletion of Access

For state staff, accounts are removed from EIM once KHRIS actions within HR are completed. Once actions are approved and completed in KHRIS, employee data is automatically sent to EIM and synced to KOG for removal. Once information is entered into KOG, the KOG account is marked as inactive.

For contract/vendor staff, accounts to be removed are requested within KOG. The KOG Administrators manually retain and enter the removal request data into EIM. Once KOG Administrators complete the process, the contract/vendor staff's domain account is marked as inactive.

4.6 External Auditor Access

All vendors/auditors must be approved, have business justification and/or agreements in place with the appropriate CHFS agencies to obtain application or network access. Only vendors/auditors deemed appropriate are approved for minimum necessary access for a defined duration of time. Vendors/auditors are bound by CHFS usage policies and procedures as well as all other federal rules and regulations. Form, CHFS-219 or CHFS-219V must be completed along with evidence of up-to-date antivirus software. External vendor access to any KOG application must follow the steps outlined in the CHFS External Auditor Access Request Procedure.

4.7 FTI Access

All FTI data access requests must follow established access request processes and be reviewed and approved by authorized personnel. Access granted to FTI data must adhere to applicable requirements in the most current version of the IRS Publication 1075.

Prior to obtaining access, employees must complete mandatory FTI training, which shall be conducted annually.

FTI access requests for individuals must follow guidelines contained in Section - 5.6 Human Services Agencies-IRC 6103(l)(7), which prohibits contractor access to FTI.

4.8 SSA Access

All access to SSA data must be approved and follow requirements within the Technical Systems Security Requirements (TSSR) control requirements. All employees that obtain access to SSA data shall complete mandatory SSA training and annually thereafter prior to obtaining access.

4.9 Offshore Access

Production data is prohibited to be accessed by any contract, state, vendor, or other personnel located offshore (outside the boundaries of the United States). All users requesting production data must be located within the United States. This applies to all CHFS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. By definition, production data is classified as “production data” when located in any environment. If production data is obfuscated, it is then not considered live production data, as such, obfuscated data may be accessed via offshore personnel.

Application source code is prohibited to be accessed by any contract, state, vendor, or other personnel located offshore (outside the boundaries of the United States). All users requesting access to application source code must be located in the United States. This applies to all CHFS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. By definition, application source code is human-readable text written in a specific programming language.

5 Policy Maintenance Responsibility

The 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 Form: CHFS External Auditor Access Request Form
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS External Auditor Access Request Procedure
- CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219)
- Enterprise IT Policy: CIO-072: IT Access Control and User Access Management Policy
- Enterprise IT Form Instructions: F181EZ- Staff Service Request, EZ Version, Form Instructions
- Enterprise IT Form: F181EZ- Staff Service Request, EZ Version, Form
- Enterprise IT Form Instructions: F181i- Staff Services Request Form Instructions
- Enterprise IT Form: F181- Staff Service Request Form (and COT Entrance/Exit Form)
- Enterprise IT Form: F085- Security Exemption Request Form
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45CFR164.308(a)(1)(ii)(A)
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- 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 800-66, Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Office of Human Resource Management (OHRM) Personnel Handbook
- Social Security Administration (SSA) Security Information