Commonwealth of Kentucky
Cabinet for Health and Family Services

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

TEAM
KENTUCKY®
CABINET FOR HEALTH
AND FAMILY SERVICES

070.206 CHFS Remote User Support Policy

Version 2.9
September 9, 2024

Revision History

Date	Version	Description	Author
9/1/2002	1.0	Effective Date	CHFS Policy Charter Team
09/09/2024	2.9	Review Date	CHFS Policy Charter Team
09/09/2024	2.9	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	9/9/2024	Jeremy Rogers	DocuSigned by: Jeremy Rogers ~~FBFD1DB52F7A404...~~
CHFS Chief Information Security Officer (or designee)	9/9/2024	Kelvin Brooks	Signed by: Kelvin Brooks A0F3F24DC182406...

Table of Contents

1 Policy Definitions

- **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 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.

- **Local Area Network (LAN):** Defined by NIST 800-82 Revision 2 as a group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.
- **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.
- **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.
- **Virtual Private Network (VPN):** Defined by NIST 800-53 Revision 4 as the protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
- **Wide Area Network (WAN):** Defined by NIST 800-82 Revision 2 as a physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive level of security controls through a CHFS Remote User Support Policy. This document establishes the agency's CHFS Remote User Support Policy, which reduces the overall risk(s), and provides guidelines for security best practices regarding remote user support.

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 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

Coordination within 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 the 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 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 Payment Card Industry (PCI), PII, ePHI, FTI and other financially sensitive information to all CHFS staff/personnel. This role, along with the CHFS 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 information system(s).

3.5 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.

3.6 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 General

COT staff has limited ability to support users of CHFS network resources that connect from remote sites that are not under the control of COT Field Services staff. This includes users from contract agencies/companies as well as users connecting from home or while traveling.

Remote Users will be responsible for a logical progression of troubleshooting as outlined below. Users should follow the steps as follows:

- Contact their Local Area Network (LAN) internet service provider to determine if their LAN and Wide Area Network (WAN) connection is properly configured and operating appropriately.
- Contact COT via the Commonwealth Service Desk at CommonwealthServiceDesk@ky.gov or by phone at (502) 564-7576 or toll-free (800) 372-7434 to ensure the remote connection hosts are operational.

To reduce CHFS liability, IT staff will not make or suggest configuration changes to remote non-CHFS equipment or service equipment at a personal residence.

CHFS staff is subject to follow all guidelines and requirements as outlined in Enterprise IT Policy: CIO-076- Firewall and Virtual Private Network Administration Policy as well as the Office of Human Resource Management (OHRM) Personnel Handbook Chapter 2.11 Telecommuting for remote user access.

4.2 Virtual Private Network (VPN)

COT staff manages all VPN services that utilize the Commonwealth of Kentucky's infrastructure. Requests for distribution lists should be submitted to CHFSServiceRequests@ky.gov. CHFS users must follow the CHFS Virtual Private Network (VPN) Procedure when requesting, accessing, removing, or taking any action to a user's VPN account.

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 Control Policy.

For any staff located within the Department for Behavioral Health, Development, and Intellectual Disabilities (BHDID) who are not on-boarded or utilizing KOG, ServiceNow shall be used to request any action (i.e., create, modify, or delete) related to CHFS domain accounts/access. Once forms are completed and approved, they must be submitted to CHFSServiceRequests@ky.gov for completion. Please refer to the COT Forms Page for instructions and more detailed information (Note: You must be connected to the state network via VPN or onsite to access the link).

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 Control Policy
- CHFS Procedure: CHFS Virtual Private Network Procedure
- Enterprise IT Policy: CIO-076- Firewall and Virtual Private Network Administration Policy
- Internal Revenue Services (IRS) Publications 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
- Office of Human Resource Management (OHRM) Personnel Handbook Chapter 2.11 Telecommuting
- Social Security Administration (SSA) Security Information