Commonwealth of Kentucky
Cabinet for Health and Family Services

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

070.400 CHFS Information Technology (IT) Standards, Policies, and Procedures (SPP) Team Charter Policy

Version 2.9
September 9, 2024

Revision History

Date	Version	Description	Author
05/2/2005	1.0	Effective Date	CHFS IT Policies Team Charter
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.
- **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.
- **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.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive level of security controls when reviewing, updating, creating, and retiring Information Technology (IT) documents, through a defined and approved Team Charter Group. This document establishes the agency's IT Standards, Policies, and Procedures (SPP) Team Charter Policy to manage risks and provide guidelines for security best practices regarding IT policy and procedure documents.

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 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 sensitive information to all CHFS staff/personnel. This role, along with the CHFS IS Team, is responsible for adherence to this policy.

3.4 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.

3.5 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 SPP Charter Team Members

Individuals designated by the division leadership to coordinate and participate in monthly meetings and discussion to improve, review, and update IT documentation. These individuals are comprised from all divisions within for input. These individuals are reviewed on an annual basis and additional staff may be added as needed for input on IT documentation.

4 Policy Requirements

4.1 General

The SPP Charter Team oversees the development and maintenance of CHFS IT standards, policies, and procedures. CHFS follows all enterprise standards, policies, and procedures as published by COT. The SPP Charter Team's objective is to establish IT documents that meet state and federal regulation requirements (i.e., NIST, CMS, IRS, SSA, etc.) through the application of enterprise and CHFS IT documents. This group is responsible for reviewing, updating, and approving IT standards, policies, and procedures. The group reviews standards on an as-needed basis while the policies and procedures are reviewed on an annual basis.

4.2 Membership of the SPP Charter Team

The SPP Charter Team is comprised of members within various divisions housed in CHFS. The SPP Charter Team members consist of staff from the following areas:

- Voting Members
  - Division of Eligibility Systems (DES) Member(s)
  - Division of Facilities Management (DFM) Member(s)
  - Division of General Accounting (DGA) Member(s)
  - Division of Application Development and Support (DADS) Member(s)
  - Division of Procurement and Grant Oversight (DPGO) Member(s)
  - Division of Social Services Systems (DSSS) Member(s)
  - Division of Health Services Systems (DHSS) Member(s)
  - Division of Strategic Services (DSS) Member(s)
  - Security and Compliance Team Member(s)
- Non-voting Administrative Organizer
- Additional Non-Voting Member(s)

SPP Charter team members are reviewed on an annual basis, or more often if needed, to ensure appropriate division personnel throughout are represented appropriately. The SPP Team Charter will review and vote/agree upon changes to the SPP group membership during this annual review. Additional staff may be a part of review/updates as deemed necessary but may not be a formal voting member. These additional staff will provide information/input to assist in ensuring IT documentation is as accurate as possible.

4.3 Frequency of Team Meetings

The SPP Charter Team meets (via teleconference, in person, or email) on a monthly basis; however, the team may elect to meet more frequently if required by the workload.

4.4 Approval Process for Document Review and Implementation

All CHFS IT policies are approved by following the process as outlined below:

- CHFS SPP Team Charter meets on a monthly basis to review, update, and comment on selected policies.

- Policies must be approved by a majority of the voting members on the SPP Charter Team.
- Policies are then reviewed and approved by a majority of the Division Directors or designee(s).
- Policies are then reviewed, approved, and signed by the CHFS CISO and/or CHFS CTO.
- Vetted and approved policies are then reviewed, approved, and signed by the IT Executive Advisor, or designee.
- The Charter Team Non-Voting Administrative Organizer is then responsible for ensuring that approved IT documents are posted to the CHFS website, the intranet, or a designated published place, as they are reviewed, approved, updated, signed, and implemented.

4.5 Review and Minor Updates to Documents

Enterprise level policies, procedures, and processes are reviewed within COT at least every two (2) to three (3) years. CHFS IS Team will annually review applicable enterprise documentation (i.e., policies, procedures, plans, etc.) for compliance. If updates are deemed necessary for updates or discussion, the IS team will bring comments to the SPP team and or management for formal suggestions or information to be provided to COT for updates that need to be made.

It is the IS team's responsibility to review all documents (i.e., policies, procedures, plans, etc.) at least once annually and maintain the documents for a minimum of six (6) years. These documents are maintained in the GRC Archer tool and in a secure folder with limited access. For major updates needed to documents, the formal SPP review process will occur. For minor updates needed to documents, the IS Team will review compliance regulations and obtain management approval for updates without having to complete the SPP formal review and approval process.

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.

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 IT Charter Team Charter Members Document
- CHFS IT Policies
- CHFS IT Standards
- CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy
- 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
- Social Security Administration (SSA) Security Information