Commonwealth of Kentucky
Cabinet for Health and Family Services

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

050.103 System's Security Plan Policy

Version 1.9
February 6, 2025

Revision History

Date	Version	Description	Author
4/29/2016	1.1	Effective Date	CHFS IT Policies Team Charter
2/06/2025	1.9	Review Date	CHFS Policy Charter Team
2/06/2025	1.9	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	2/6/2025	Jeremy Rogers	DocuSigned by: Jeremy Rogers FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or delegate)	2/6/2025	Kelvin Brooks	Signed by: Kelvin Brooks A0F3F24DC182406...

Table of Contents

1 POLICY DEFINITIONS 4

2 POLICY OVERVIEW 7

2.1 PURPOSE 7
2.2 SCOPE 7
2.3 MANAGEMENT COMMITMENT 7
2.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES 7
2.5 COMPLIANCE 7

3 ROLES AND RESPONSIBILITIES 8

3.1 CHIEF INFORMATION SECURITY OFFICER (CISO) 8
3.2 CHIEF PRIVACY OFFICER (CPO) 8
3.3 CHIEF/ DEPUTY CHIEF TECHNOLOGY OFFICER (CTO) 8
3.4 SECURITY/PRIVACY LEAD 8
3.5 CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL 8
3.6 SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS 8
3.7 CHFS SECURITY RISK MANAGER 9

4 POLICY REQUIREMENTS 9

4.1 SYSTEM SECURITY PLAN 9

4.2 RULES OF BEHAVIOR 10

4.3 INFORMATION SECURITY ARCHITECTURE 11

5 POLICY MAINTENANCE RESPONSIBILITY 11
6 POLICY EXCEPTIONS 11
7 POLICY REVIEW CYCLE 11

8 POLICY REFERENCES 11

1 Policy Definitions

- **Agency:** Defined by CHFS for the purpose of this document, agency or agencies refers to any department within CHFS.
- **Authorization Boundary:** All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
- **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 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} IT Staff Augmentation contract 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 includes 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 the 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.
- **Risk:** Defined by NIST SP 800-30 as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information System security related risk is one that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation.
- **Risk Assessment:** Defined by NIST SP 800-30 as the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
- **Rules of Behavior:** Defined by CHFS as security control contained in NIST SP 800-53, should clearly delineate responsibilities, and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for access to the system. It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior.
- **Security (Control) Assessment:** Defined by NIST 800-53 Revision 4 as the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
- **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.

- **Sensitive Financial Data (including PCI):** Defined by Payment Card Industry (PCI) Data Security Standards (DSS) Security Standards as cardholder and sensitive authentication data including Primary Account Number (PAN), cardholder name, expiration date, service code, full track data (magnetic stripe data or equivalent on a chip0, Card Security Codes such as CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data as anything that is inclusive of bank identification/information (i.e., bank routing number, account number, etc.).
- **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 played by a CHFS Branch Manager.
- **System/Data Owner:** Defined by CHFS as an individual who has final agency responsibility of data protection and is the person held responsible 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, usually a senior executive, designates the confidentiality of the system/data, 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 played by a CHFS Business Executive.
- **Third Party:** Defined by CHFS as any contracted or government organization that is not a part of the agency's organizational structure. This may include state or federal auditing agencies, state approved security contract vendors or other external organization whose capabilities can be determined sufficient to conduct assessment needs.
- **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) must establish a comprehensive level of security controls through a security planning policy. This document establishes the System's Security Planning Policy which helps manage risks and provides guidelines for security best practices regarding security planning, preparation, and strategy.

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

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 NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within CMS, 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) self-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

Individuals are designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of PII, ePHI, FTI and other financial sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS IS team is responsible for the adherence of 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 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.

3.7 CHFS Security Risk Manager

This position is responsible for the governance of the overall risk assessment program within the Cabinet. This role will provide guidance to program areas in the assessment and identification of potential risks. They will inform, coordinate, and assist the System Data Owner in documenting the risks and successfully completing the assessment.

The Risk Manager will maintain communication with the System Data Owner and ensure that the schedule of upcoming security control assessments is conveyed so that timely submissions of the assessments are met and completed. The Risk Manager works with the System Data Owner to address all risks based on NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, for moderate baseline requirements.

4 Policy Requirements

4.1 System Security Plan

CHFS and vendor developed agency information systems must create and maintain a System Security Plan (SSP). Per IRS guidelines, an approved System Security Report (SSR) satisfies the SSP requirement for applications that receive, process, store, or transmit FTI.

The System Security Plan (SSP) must define the roles, responsibilities, and expected behavior of individuals accessing the information system to ensure compliance with security policies and best practices The SSP/SSR shall be viewed as documentation and processes for the security protections of information systems, including those that contain FTI.

The agency must develop a system security plan that includes, but is not limited to, the following guidelines:

1. A plan that is consistent with the organization's enterprise architecture.
2. A plan that explicitly defines the authorization boundary for the system.
3. A plan that describes the operational context of the information system in terms of missions and business processes.
4. A plan that provides the security categorization of the information system, including supporting rationale.
5. A plan that describes the operational environment for the information system and relationships with or connections to other information systems.
6. A plan that provides an overview of the security requirements for the system
7. A plan that identifies any relevant overlays, if applicable.
8. A plan that describes the security controls in place or planned for meeting those requirements, including a rationale for tailoring decisions.

9. A plan that is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
10. A plan that enables the CHFS IS Team to conduct ongoing security control assessments to assess CHFS' current state security posture and assure alignment with applicable requirements.
11. A plan that ensures assessments are in accordance with Regulatory Mandates and the CHFS continuous monitoring strategy.

12. A plan that utilizes checklist assessments (as subsets of baseline NIST controls) to assess a finite number of key controls.
13. A plan that provides a high-level, strategic view of the CHFS management of cybersecurity risk.
14. A plan that measures and improves cybersecurity performance at various organizational levels.
15. A plan that enhances communication concerning cybersecurity risk, activities, and results across the CHFS-wide risk management program.
16. A plan that aligns and prioritizes cybersecurity requirements for use in the acquisition process and to inform management of the tailoring of controls.

The SSP/SSR will be reviewed at least annually or more often if there are major system changes or a significant change in the environment. The agency will share the plan updates and changes with all necessary agency management staff as needed or upon request. An example/template of how to create an Information System Security Plan can be found in Appendix A of the NIST Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems: Appendix A.

Reasons for changes or updates to the plan may include, but are not limited to:

1. Changes to the information systems.
2. Change to the environment of operations.
3. Change or updates to security controls in place.
4. Problems identified during plan implementations or security control assessments.
5. Other major releases or changes to the system or application.

Agencies may develop procedures to plan and coordinate security related activities regarding the information system with affected stakeholders before conducting such activities to reduce the impact on other organizational entities.

4.2 Rules of Behavior

CHFS establishes, provides, describes, and makes readily available the responsibilities and expected behavior of individuals who require access to the information system.

Upon employment and prior to system access, individuals are required to sign a "Rules of Behavior" acknowledgment form, such as the CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS 219).

4.3 Information Security Architecture

The agency will develop the information security architecture for the information system. This architecture will describe the overall requirements of how the agency plans to protect the confidentiality, integrity, and availability of the information. This security architecture will be updated annually or when significant changes occur to reflect updates in the enterprise architecture. All changes and updates will be documented in the SSP/SSR when applicable.

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 annually and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.2
- CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS 219)
- CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy
- CHFS Procedure: CHFS System's Security Plan Procedure
- CIO-091: Enterprise Information Security Program
- CIO-115: Physical and Environmental Protection Policy
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statue (KRS) Chapter 61: House Bill 5 (HB5)
- National Institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Payment Card industry (PCI) data Security Standard (DSS) Requirements and

Security Assessment Procedures Version 3.2.1

- Social Security Administration (SSA) Security Information
- U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)