Commonwealth of Kentucky
Cabinet for Health and Family Services

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

080.101 AI/Gen AI Policy

Version 1.1
February 27, 2025

Revision History

Date	Version	Description	Author
01/08/2024	1.0	Effective Date	CHFS Policy Charter Team
02/27/2025	1.1	Review Date	CHFS Policy Charter Team
02/27/2025	1.1	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	2/27/2025	Jeremy Rogers	DocuSigned by: Jeremy Rogers FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or designee)	2/27/2025	Kelvin Brooks	Signed by: Kelvin Brooks A0F3F24DC182406...

Table of Contents

1 Policy Definitions

- **AI (Artificial Intelligence)**: Systems that simulate human intelligence processes, including learning, reasoning, and self-correction. AI is the field of computer science and technology that focuses on creating systems capable of performing tasks that typically require human intelligence, which includes, but is not limited to, machine learning, large language models, reinforcement learning, natural language processing, computer vision and deep learning.
- **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/CHFS) vendor who has a master agreement with the state.
- **Discovery:** Defined by CHFS as manually walking through the web application to understand the logic and operational flows in order to filter out information that may generate messages or emails triggered by scanning.
- **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.
- **Generative AI**: Generative Artificial Intelligence (AI) is a technology that can create content, including text, images, audio, or video, when prompted by a user. Generative AI systems learn patterns and relationships from massive amounts of data, which enables them to generate new content that may be similar, but not identical, to the underlying training data. The systems generally require a user to submit prompts that guide the generation of new content.
- **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.

- **Manual Penetration Test:** Defined by CHFS as the process of examining specific flaw categories that currently require manual inspection to evaluate the security of the infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations, or risky end-user behavior.
- **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.
- **Security Review:** Defined by CHFS as a security assessment which will end with a list of all vulnerabilities that are found through the web. Risk should be prioritized based on the ease of exploiting the vulnerability and the potential harm that could result if an attacker is successful. The results will be disseminated to the project team, who will then prioritize what needs to be fixed so that existing applications can be hardened. Those applications being built can be remedied and safely placed into production.
- **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 an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.
- **Vulnerability Assessment:** Defined by NIST SP 800-30 as systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
- **Vulnerability Scan:** Defined by CHFS as an execution of automated security scanning software that attempts to discover, define, identify, and classify the lapse in security in a web application or network system. This automated vulnerability scan is considered intrusive.

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 application and security controls through a system technical assessment policy. This document establishes general policies to govern usage of Artificial Intelligence (AI)/Generative AI in the Cabinet.

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 related to AI/Gen AI.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), CHFS Deputy 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 the National Institute for Standards and Technology (NIST) AI Risk Management Framework. Additionally, applicable agencies follow security and privacy frameworks outlined within the CMS, the IRS, and the SSA.

3 Roles and Responsibilities

3.1 Chief/ Deputy Chief Technology Officer (CTO)

This individual makes decisions related to a CHFS technology strategy. 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 policy.

3.2 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.

3.3 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 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.

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

4 Policy Requirements

CHFS believes that the rapid advancement of AI, especially generative artificial intelligence (Gen AI), has the potential to transform CHFS business processes and ultimately improve efficiency. CHFS is aware that these technologies also pose new and challenging considerations for implementation. This policy provides guidelines to enforce the responsible use of AI/Gen AI to foster public trust, support business outcomes, and ensure the ethical, transparent, accountable, and responsible implementation of this technology.

Recognizing the rapidly evolving nature of AI, this policy will need to be periodically reviewed on a bi-annual basis and updated to align with emerging state and federal regulations/guidelines, technologies, and use cases. CHFS shall establish an AI Governance Committee for use case intake, monitoring, guidance, and policy enforcement and maintain an AI project inventory to track and assess all ongoing and proposed AI initiatives.

This policy applies to the use of AI, including GenAI applications, or the development of GenAI models, including internal models, third party models, or publicly available applications such as ChatGPT. This policy applies to the use of those applications on CHFS devices and/or personal devices when used for work purposes.

4.1 *AI/Gen AI Usage Guidelines*

- Accountability and Oversight:

  A mechanism for human review shall exist for all AI-driven decisions. Generative AI models shall have a human-in-the-loop for quality assurance.

- Fairness and Transparency:

  - AI systems shall be designed to provide consistent and similar quality of service for all users.
  - AI applications shall maintain transparency in their decision-making processes. For generative AI outputs, metadata shall be kept for traceability and shall provide context and references from where the information was pulled to allow for verification and validation.

- Security and Reliability:

  - Adherence to state and federal security policies and standards is mandatory.
  - Strong security protocols shall be in place to prevent unauthorized access and manipulation of AI systems. AI systems shall be routinely tested for robustness and reliability.

  - To maintain the security of our data and IT systems, employees are prohibited from attempting to gain access to unapproved GenAI applications when using CHFS systems or networks, conducting business on behalf of the CHFS, or accessing CHFS data.

- Disclosure:

  - When generative AI is used, especially in communications, its use shall be disclosed.

- Ethical Considerations

  - Fairness: All AI models, including generative, shall be trained and tested for biases and shall not perpetuate discrimination.
  - Integrity: Ensure AI systems act in ways that are understandable and traceable.
  - Systems/ users shall review the output of GenAI applications to make sure they meet CHFS's standards for principles of equity, ethics, and appropriateness.
  - Systems/ users shall not use GenAI applications to create text, audio, or visual content for purposes of committing fraud or misrepresenting an individual's identity.

- Data Handling:

  - Adherence to Commonwealth Office of Technology metadata/ data retention, protection, and privacy policies is mandatory.
  - Systems/ Users shall only share information with approved personnel and only input approved data into approved GenAI systems.
  - All AI projects shall ensure appropriate data classification and handling, compliance with data privacy requirements, establish clear data ownership and responsibility, document data lineage and usage permissions, monitor and prevent unauthorized data exposure
  - All data flow requirements for AI/Gen AI implementations shall be reviewed with Cabinet AI governance, security teams.

- Risk management

  AI risk management is a key component of the responsible development and use of AI systems, and teams must employ comprehensive risk and threat management controls based on defined industry standards like the NIST AI risk management framework to develop Responsible AI practices to enhance trustworthiness and adoption.

- Incident Reporting

  Cabinet AI systems and associated vendors shall define a clear mechanism for reporting AI-related concerns or incidents that follows CHFS reporting standards and policies. Please notify the CHFS Incident Response Team at CHFSIncidentResponse@ky.gov and copy the CHFS Security Team at CHFSOATSSecurity@ky.gov.

- Monitoring

  - Regular audits of AI projects to ensure ethical use and policy adherence. Any deviations should be reported to the AI governance board.
  - All CHFS users are expected to comply with applicable laws, regulations, and Commonwealth policies regarding the use or development of GenAI content or tools.

- Training and Awareness

  All personnel involved in AI projects, directly or indirectly, shall review this policy as part of project onboarding and account for policy requirements as part of their project SDLC. CHFS works with vendors to develop and provide AI related training and awareness activities for all staff and contractors using AI related software.

- Organizational Change Management

  To drive a successful change, teams shall establish a thorough OCM strategy to help foster the right employee mindset and behaviors needed for successful AI implementation.

- Usage and Adoption Considerations:
  - Consistent with the CHFS Technology Acquisition Policy, CHFS teams are authorized to use pre-approved GenAI software tools, or they may request a non-standard acquisition of GenAI software. This applies to all technology, including free-to-use software or software-as-a-service tools.
  - All CHFS Gen AI implementations, including 3rd party products leveraging AI as part of their product, are subject to CHFS AI Governance Board approval.
  - Use cases that will be considered for CHFS AI Governance Board approval:
    - Do not encompass sensitive or confidential information, including but not limited to PHI/ PII.
    - Targeted for internal audiences.
    - Any other use cases like for example that are public facing or include sensitive or confidential information, including but not limited to PHI/ PII will be reviewed and approved as exceptions only.

- CHFS's AI Governance team may revoke authorization for a technology that adds AI capabilities or may restrict the use of those AI capabilities if, in its judgment, those AI capabilities present risks that cannot be effectively mitigated to comply with CHFS policies.
- All generative AI implementations shall include a verification/validation phase by a qualified subject matter expert (SME) in the loop before implementation to production.
- All cabinet implementations including vendor solutions should demonstrate the Gen AI capabilities leveraged by the proposed research and analytics platform to improve the business outcomes. Usage of Gen AI should adhere to the guidelines to enforce responsible use of Gen AI in the CHFS AI policy. Applications shall provide ability to enable or disable AI technologies and CHFS may revoke authorization or may restrict the use of those AI capabilities, if, in its judgment, those AI capabilities present risks that cannot be effectively mitigated to comply with CHFS policies.
- Cabinet AI implementations shall undergo comprehensive validation and testing processes to ensure reliability, security, and performance prior to deployment and throughout their lifecycle.
- CHFS Divisions must provide an inventory of all applications currently in use, under development, or in initial discovery phases within their division that include, either in whole or in part, an AI/ Generative AI solution. Reporting will be in a manner prescribed by CHFS AI Governance team.

- Tools and Software:
  - All tools and software procured for production AI based implementations will need to be validated and approved by CHFS and align with CHFS Technology Acquisition Policy.
  - Cabinet in collaboration with COT is currently evaluating M365, GitHub copilots.
  - Please contact CHFS_AIGovGroup@ky.gov for any questions in the meantime.

4.2 CHFS AI Governance team:

Below is a high-level representation of the AI Governance team. A separate charter with detailed roles and activities is under development. Please contact CHFS_AIGovGroup@ky.gov for any questions in the meantime.

Role	Activities
Security and Compliance Team	• Develop and manage the GenAI security policy. • Support IT Security incident response resulting from the use of GenAI.

	• Conduct security risk assessments for GenAI applications and use cases.
Privacy Team	• Conduct privacy risk assessment for GenAI applications and use cases.
CHFS AI Governance team	• Conduct a review of specific uses of GenAI • Review and approve/ reject GenAI applications. • Review all GenAI output for bias, accuracy, and appropriateness. • Review and approve/ reject software and tools. • Review and approve/ reject Models based on the use case. • Review and approve/ reject the deployment approach. • Review policies and procedures on an annual basis (i.e., mandatory training).

5 Policy Maintenance Responsibility

The CHFS AI Governance team is responsible for the maintenance of this policy. Recognizing the rapidly evolving nature of AI, these guidelines will need to be periodically reviewed on a bi-annual basis and updated to align with emerging state and federal guidelines, technologies, challenges, and use cases.

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 bi-annually and revised on an as needed basis.

8 Policy References

- CHFS Policy: 070.110 Technology Acquisition Policy
- NIST AI risk management framework:
  Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov)
- Trustworthy AI (TAI) Playbook
  HHS Trustworthy Artificial Intelligence (AI) Playbook (09/30/2021)

- AI Guide for Government
  AI Guide for Government - AI CoE (gsa.gov)
- AI Strategy and use cases
  HHS Artificial Intelligence (AI) Strategy | HHS.gov
- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.2
- CHFS Policy: 070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS Procedure: CHFS Systems Development Lifecycle (SDLC) and New Application Development Procedure
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Internal Revenue Services (IRS) Publication 1075
- Information Technology Management Portal (ITMP)
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- 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 800-64 Revision 2, Security Considerations in the System Development Life Cycle
- Generative AI Guidelines | OCIO (wa.gov)
- White House Executive Order on Safe Secure and Responsible Use of AI
- Commonwealth Office of Technology Policies
- CHFS IT Policies - Cabinet for Health and Family Services (ky.gov)
- Privacy- CHFS Collection, Use, and Retention of Personal Information.pdf (ky.gov)