



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



020.205 IT System Technical Assessments Policy

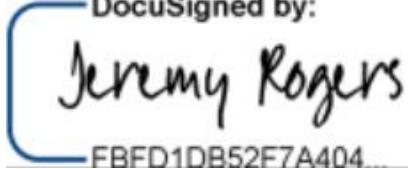
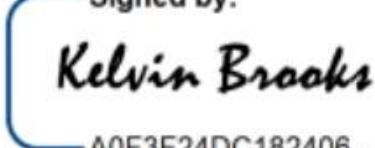
Version 2.8
October 4, 2024

020.205 IT System Technical Assessments Policy	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

Revision History

Date	Version	Description	Author
05/02/2005	1.0	Effective Date	CHFS IT Policies Team Charter
10/04/2024	2.8	Review Date	CHFS Policy Charter Team
10/04/2024	2.8	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	10/04/2024	Jeremy Rogers	DocuSigned by:  FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or designee)	10/04/2024	Kelvin Brooks	Signed by:  A0F3F24DC182406...

<u>020.205 IT System Technical Assessments Policy</u>	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

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 TECHNICAL OFFICER (CTO).....	8
3.4	SECURITY/PRIVACY LEAD	8
3.5	CHIEF/ DEPUTY CHIEF TECHNOLOGY OFFICER (CTO).....	8
3.6	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	8
3.7	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	9
4	POLICY REQUIREMENTS	9
4.1	GENERAL	9
4.2	SECURITY IT STAFF RESPONSIBILITY.....	10
4.3	ASSESSMENTS DETAILS	10
5	POLICY MAINTENANCE RESPONSIBILITY	10
6	POLICY EXCEPTIONS	10
7	POLICY REVIEW CYCLE.....	10
8	POLICY REFERENCES	10

020.205 IT System Technical Assessments Policy	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

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.
- **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 email 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.
- **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

020.205 IT System Technical Assessments Policy	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

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 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 a formal contract such as the System Design/Development Services (SDS) contract or other approved 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

<u>020.205 IT System Technical Assessments Policy</u>	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

security in a web application or network system. This automated vulnerability scan is considered intrusive.

020.205 IT System Technical Assessments Policy	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive level of security controls through a system technical assessment policy. This document establishes the agency's Information Technology (IT) System Technical Assessments to manage risks and provide guidelines for security best practices regarding the agency's IT assessments.

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

CHFS organizations and/or agencies that access applications, systems, and facilities work in coordination to ensure requirements outlined in this policy are followed.. 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 the SSA.

020.205 IT System Technical Assessments Policy	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

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 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 Chief/Deputy Technical 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

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 IS Team is responsible for adherence to this policy.

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 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).

020.205 IT System Technical Assessments Policy	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

3.7 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

CHFS complies with and adheres to COT Enterprise policies. CHFS works collaboratively with program areas to determine the level of sensitivity of its data.

The CHFS executive leadership, along with business partners and other stakeholders, shall define the agency's mission critical systems that are subject to meet the assessments listed and defined within this policy. All other agency systems containing sensitive data, but not deemed mission critical should also comply with IT Technical assessment requirements outlined in this policy.

CHFS utilizes the NIST federal standards as well as [Federal Information Processing Standards \(FIPS\) Publication 199](#), Standards for Security Categorization of Federal Information and Information Systems for determining its critical systems. Utilizing FIPS 199, a system is defined as critical when the potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

CHFS also follows [065.014 CHFS Software Development Lifecycle \(SDLC\) and New Application Development Policy](#) and [CHFS 040.201 Internal Risk Assessment Policy](#). Vulnerability assessments related to these policies can be performed by the internal CHFS IS Team or contracted to an approved third-party vendor.

020.205 IT System Technical Assessments Policy	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

4.2 Security IT Staff Responsibility

The CHFS IS Team is responsible for overseeing the vulnerability assessments of each system covered by this policy. If the agency decides to use a third-party vendor, the CHFS IS Team is responsible for ensuring the third-party vendor is qualified and approved by CHFS management. For internal and third-party assessments that the CHFS IS Team is notified of, the IS Team will maintain a list of assessments performed. This list will identify the assessment performed, the application assessed, the date(s) of the assessment or retesting, and the party performing the assessment. The CHFS IS Team is responsible for updating this policy, as well as associated procedures, when changes to the infrastructure or enterprise environment occur.

4.3 Assessments Details

CHFS IS Team utilizes a layered approach methodology to application security testing. The methodology for this assessment includes Discovery, Vulnerability Scanning, Manual Penetration Testing, Vulnerability Assessments, and Security Reviews.

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 Policy: 040.201 Internal Risk Assessment Policy](#)
- [CHFS Policy: 065.014 CHFS SDLC and New Application Development Policy](#)
- [CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy](#)
- [CHFS Procedure: CHFS Risk Assessment Program Procedure](#)
- [Federal Information Processing Standards \(FIPS\) Publication 199](#)
- [Internal Revenue Services \(IRS\) Publication 1075](#)
- [Kentucky Information Technology Standards \(KITS\): 4080 Data Classification](#)

<u>020.205 IT System Technical Assessments Policy</u>	Current Version: 2.8
020.200 Managerial Security	Review Date: 10/04/2024

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
- Social Security Administration (SSA) Security Information