



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



CHFS

KENTUCKY
*Cabinet for Health and
Family Services*

020.206 Certification and Accreditation Policy



Version 2.5
June 18, 2021

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

Revision History

Date	Version	Description	Author
12/16/2011	1.0	Effective Date	CHFS IT Policies Team Charter
6/18/2021	2.5	Review Date	CHFS OATS Policy Charter Team
6/18/2021	2.5	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	6/18/2021	Jennifer Harp	DocuSigned by:  057B913AA3E14AE...
CHFS Chief Information Security Officer (or designee)	6/18/2021	Nicholas Tomlin	DocuSigned by:  55B6A12812DD403...

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

Table of Contents

1	POLICY DEFINITIONS	4
2	POLICY OVERVIEW	6
2.1	PURPOSE	6
2.2	SCOPE	6
2.3	MANAGEMENT COMMITMENT	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	6
2.5	COMPLIANCE.....	6
3	ROLES AND RESPONSIBILITIES	6
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	6
3.2	CHIEF PRIVACY OFFICER (CPO)	7
3.3	SECURITY/PRIVACY LEAD.....	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
4	POLICY REQUIREMENTS	7
4.1	GENERAL INFORMATION	7
4.2	SECURITY ASSESSMENTS	8
4.3	PLAN OF ACTION AND MILESTONES (POA&M).....	8
4.4	RESPONSIBILITY	8
4.5	COMPLETION AND APPROVAL PROCESS	8
5	POLICY MAINTENANCE RESPONSIBILITY	8
6	POLICY EXCEPTIONS	8
7	POLICY REVIEW CYCLE	9
8	POLICY REFERENCES	9

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

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

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

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 an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

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 security controls through a certification and accreditation policy. This document establishes the agency's Certification and Accreditation Policy to manage risks and provide guidelines for security best practices regarding the review and appropriate maintenance of the agency's information system.

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

OATS 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

OATS 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 the NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within 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.

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

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 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.

3.3 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 protection of 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.

3.4 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/OATS information system(s).

3.5 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 Information

CHFS will certify and accredit annually any information system within OATS that employs sensitive information. Certification, accreditation, and security/risk assessments will be used to ensure appropriate levels of controls exist and that they are managed, and compliant with all federal and state laws and regulations. CHFS will ensure that the most current baseline security requirements are met as defined by the latest version of the NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

4.2 Security Assessments

All critical applications, as defined by CHFS leadership, business partners, and other stakeholders, will undergo a partial or full security and privacy assessment, per the [NIST 800-53 Revision 4](#) guidelines. A report will be generated subsequently with the assessment results. The assessment will be reviewed and approved by the appropriate system data owner and/or system data administrator and results will be shared with parties deemed appropriate.

4.3 Plan of Action and Milestones (POA&M)

A Plan of Action and Milestones (POA&M) will be developed for all critical applications, as defined by CHFS leadership, business partners, and other stakeholders per the [NIST 800-53 Revision 4](#), [Minimum Acceptable Risk Standards for Exchanges \(MARS-E\)](#), or other guidelines as applicable. Findings and corrections, based on any audits, security impact analyses, monitoring activities, or other review types, shall be documented and tracked in the Agency's POA&M. This will reduce or eliminate known vulnerabilities in the system.

The POA&M must be monitored and updated as needed on a regular basis. Please refer to the [CHFS Plan of Action and Milestone \(POA&M\) Procedure](#) established for agencies that report to the IRS or CMS for more actions.

4.4 Responsibility

The OATS IS Team is responsible for oversight of vulnerability assessments of each system covered by this policy. If a third party is used, the OATS IS Team is responsible for ensuring that the vendor is qualified, as determined by COT.

4.5 Completion and Approval Process

The certification and accreditation process is performed by the OATS IS team. A senior level executive or manager will be appointed to authorize each agency's information system. The appointed executive or manager will validate the information system is approved before commencing operations.

This policy also aligns with all OATS and COT Enterprise policies pertaining to Data/Media Security.

5 Policy Maintenance Responsibility

The OATS 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 OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy](#).

020.206 Certification and Accreditation	Current Version: 2.5
020.200 Managerial Security	Review Date: 06/18/2021

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 2.0](#)
- [CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy](#)
- [CHFS OATS Procedure: CHFS Plan of Action and Milestone\(POA&M\) Procedure](#)
- [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](#)
- [Minimum Acceptable Risk Standards for Exchanges \(MARS-E\)](#)
- [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](#)