Commonwealth of Kentucky
Cabinet for Health and Family Services

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

CHFS
KENTUCKY
Cabinet *for* Health *and* Family Services

065.015 Application Audit and Accountability (AU) Policy

Version 2.5
February 24, 2021

Revision History

Date	Version	Description	Author
2/23/2011	1.0	Effective Date	CHFS IT Policies Team Charter
2/24/2021	2.5	Review Date	CHFS OATS Policy Charter Team
2/24/2021	2.5	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	2/24/2021	Jennifer Harp	DocuSigned by: Jennifer Harp 057B913AA3E14AE...
CHFS Chief Information Security Officer (or delegate)	2/24/2021	Nicholas Tomlin	DocuSigned by: 55B6A12812DD403...

Table of Contents

1 Policy Definitions

- **Audit Log Failure**: Defined by CHFS as events defined by federal and state guidelines in which logs being captured show issues or errors. Audit log failures can include but are not limited to: software/hardware errors, failures in the audit capturing mechanisms, audit storage capacity being reached or exceeded, location of access, and severity of captured information.
- **Auditable Events**: Defined by CHFS as events defined by federal, state, and agency guidelines, needing to be audited and retained by the agency for the defined period of time. Auditable events can include but are not limited to: number of failed system log-on attempts, password changes, system errors, printing, changes, updates, deletions to the system, and application errors.
- **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} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Coordinated Universal Time (UTC):** Defined by CHFS as the time standard commonly used across the world, basis for civil time today. Unlike GMT, UTC is the world time standard and is not a time zone. This 24-hour time standard is kept using highly precise atomic clocks combined with Earth's rotation.
- **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.

- **Greenwich Mean Time (GMT):** Defined by CHFS as the time zone used by Europe and other countries. The standard GMT is the same time as UTC, neither change for Daylight Saving Time.
- **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.
- **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.

- **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) Office of Application Technology Services (OATS) must establish a comprehensive level of security controls through an audit and accountability policy. This document establishes the agency's Application Audit and Accountability Policy, which helps manage risks and provides guidelines for security best practices regarding audit record retention

2.2 Scope

The scope of this policy applies to business owners or designees that my include 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. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

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, 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 CHFS OATS Information Security (IS) Team

The CHFS OATS IS team is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required.

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 Health Insurance Portability and Accountability Act (HIPAA) risk assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS 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

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 the protection of PCI, PII, ePHI, FTI and other financially sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS 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 procedure. 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

4.1 Auditable Events

The agency designee will ensure that the information system or components are capable of auditing events defined by federal and state regulations. The agency designee will coordinate security functions and controls with other organizational entities to ensure required auditable events or related data are being captured. CHFS shall follow the CHFS Audit and Accountability Procedure for additional information on audit logs, events, and more.

4.2 Content of Auditable Events

The information system will generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

4.3 Audit Storage Capacity

The agency will allocate audit storage capacity in accordance with all federal and state regulations and guidance.

4.4 Response to Audit Processing Failures

The information system and/or its components will alert designated agency personnel in the event of an audit log failure where agency action will then be taken.

4.5 Audit Review, Analysis, and Reporting

The CHFS IS team will work with System Data Owners, or delegate(s), who receive and analyze audits and reports, as directed by federal and state regulations. Findings of the reviewed information system audit records, and or issues, will be reported to management.

4.6 Audit Reduction and Report Generation

The information system provides an audit reduction report generation capability that supports functions for on demand audit review, analysis and reporting requirements, and after the fact investigation of security incidents. The information system will not alter the original content or time ordering of any audit records.

4.7 Time Stamps

Information systems will use internal system clocks that can be mapped to Coordinated Universal Time (UTC) to generate time stamps. The agency will meet federal and state defined granularity of time measurements on audit logs.

4.8 Protection of Audit Information

Audit information will be protected from unauthorized access, modifications and deletions. The agency will have compensating controls in place to prevent any unauthorized action to be taken on audit information.

4.9 Audit Record Retention

The agency will retain audit records to provide support for after the fact investigations of security incidents and to meet all state and federal regulatory retention requirements. Agencies will follow CHFS 040.101- Application Backup Policy.

4.10 Audit Generation

Auditable events will be generated by the information system. Agency personnel may have the ability to select which events are to be audited.

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.

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 2.0
- CHFS OATS Policy: 040.101- Application Backup Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Audit and Accountability Procedure
- 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 800-53 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)