

Commonwealth of Kentucky
Cabinet for Health and Family Services



Information Technology (IT) Policy



065.015 Application Audit and Accountability

Version 2.1
February 29, 2016

065.015 Application Audit and Accountability	Current Version: 2.1
065.000 Application Development	Effective Date: 02/23/2011

Revision History

Date	Version	Description	Author
02/23/2011	1.0	Effective Date	CHFS IT Policies Team Charter
2/29/2016	2.1	Revision Date	CHFS IT Policies Team Charter
2/29/2016	2.1	Review Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Executive Director (or designee)	2/29/2016	Bernard Decker	

065.015 Application Audit and Accountability	Current Version: 2.1
065.000 Application Development	Effective Date: 02/23/2011

Table of Contents

1	065.015 APPLICATION AUDIT AND ACCOUNTABILITY	4
1.1	PURPOSE	4
1.2	SCOPE	4
1.3	ROLES AND RESPONSIBILITIES	4
1.3.1	<i>Security Lead</i>	4
1.3.2	<i>Privacy Lead</i>	4
1.3.3	<i>CHFS Staff</i>	4
1.4	MANAGEMENT COMMITMENT	4
1.5	COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.6	COMPLIANCE	5
2	POLICY REQUIREMENTS	5
2.1	AUDITABLE EVENTS	5
2.2	CONTENT OF AUDITABLE EVENTS	5
2.3	AUDIT STORAGE CAPACITY	5
2.4	RESPONSE TO AUDIT PROCESSING FAILURES	5
2.5	AUDIT REVIEW, ANALYSIS, AND REPORTING	5
2.6	AUDIT REDUCTION AND REPORT GENERATION	6
2.7	TIME STAMPS.....	6
2.8	PROTECTION OF AUDIT INFORMATION	6
2.9	AUDIT RECORD RETENTION.....	6
2.10	AUDIT GENERATION	6
2.11	DEFINITIONS	6
2.11.1	<i>Confidential Informaiton</i>	6
2.11.2	<i>Auditable Events</i>	6
2.11.3	<i>Audit Log Failure</i>	7
3	POLICY MAINTENANCE RESPONSIBILITY	7
4	EXCEPTIONS	7
5	POLICY REVIEW CYCLE	7
6	REFERENCES	7

065.015 Application Audit and Accountability	Current Version: 2.1
065.000 Application Development	Effective Date: 02/23/2011

1 065.015 Application Audit and Accountability

Category: 065.000 Application Development

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Service (OATS) must establish an acceptable level of security controls to be implemented through an audit and accountability policy. This document establishes the agency's Application Audit and Accountability Policy which help manage risks and lays out guidelines for implementing security best practices in regards to audit record retention.

1.2 Scope

The scope of this policy applies to all CHFS OATS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. This policy covers the applicable computer and data communication systems owned and administered by CHFS OATS or third party providers under contract with a CHFS agency.

1.3 Roles and Responsibilities

1.3.1 Security Lead

Responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This role is responsible for the adherence of the Application Audit and Accountability Policy.

1.3.2 Privacy Lead

Responsible to provide the security and privacy guidance of sensitive information to all CHFS information technology (IT) staff. This role is responsible for the adherence of the Application Audit and Accountability Policy alongside the Security Lead.

1.3.3 CHFS Staff

Responsible to adhere to the Application Audit and Accountability Policy as well as referenced documents that pertain to the agency's applications.

1.4 Management Commitment

This policy has been approved by OATS Division Directors and the OATS Executive Director. Senior Management supports the objective put into place by this policy.

065.015 Application Audit and Accountability	Current Version: 2.1
065.000 Application Development	Effective Date: 02/23/2011

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet who access their applications or systems. All organizational entities that interact with OATS are subject to follow guidelines outlined within this policy.

1.6 Compliance

CHFS has chosen to adopt the security awareness and principles established in the National Institute of Standards and Technology (NIST), the Internal Revenue Services (IRS), the Social Security Administration (SSA), the Centers for Medicare and Medicaid Services (CMS), as well as other federal and state organizations as the official guidance domain for this policy.

2 Policy Requirements

2.1 Auditable Events

The agency will ensure that the information system or components are capable of auditing events defined by federal and state regulations. The agency will coordinate security functions and controls with other organizational entities to ensure required auditable events or related data are being captured.

2.2 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.

2.3 Audit Storage Capacity

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

2.4 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.

2.5 Audit Review, Analysis, and Reporting

The agency designate official(s) whom receive audit reports will regularly, as directed by federal and state regulations, review and analyze the information system audit records and report issues or findings to management.

065.015 Application Audit and Accountability	Current Version: 2.1
065.000 Application Development	Effective Date: 02/23/2011

2.6 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.

2.7 Time Stamps

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

2.8 Protection of Audit Information

The information system will protect audit information and audit tools from unauthorized access, modifications, and deletion capabilities. The agency will have compensating controls in place to prevent any unauthorized action to be taken on audit information.

2.9 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 IT Policy: 040.101 Server/Application Backup and Retention Policy.

2.10 Audit Generation

The information system will provide audit record generation capability for the auditable events and allow designated agency personnel to select which audible events are to be audited by specific components of the information system.

2.11 Definitions

2.11.1 Confidential Information

Any information that pertains to identifying a person by name, address, social security number, or other forms of personal identification; including Protected Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information (FTI) or Internal Revenue Services (IRS) provided Data, Social Security Administration (SSA) provided Data, Centers for Medicare and Medicaid Services (CMS) provided data, Health Insurance Portability and Accountability Act (HIPAA) provided data, and other federally provided personal data.

2.11.2 Auditable Events

Events defined by federal agency guidelines, needing to be audited and retained by the agency for a defined period of time. Auditable events can include but is not limited to the following:

065.015 Application Audit and Accountability	Current Version: 2.1
065.000 Application Development	Effective Date: 02/23/2011

- Number of failed system log-on attempts
- Password changes
- System errors
- Printing
- Changes, updates, deletions made to the system
- Application errors

2.11.3 Audit Log Failure

Events defined by federal and state guidelines in which logs being captured are show issues or errors. Audit Log Failures can include but are not limited to the following:

- Software/hardware errors
- Failures in the audit capturing mechanisms
- Audit storage capacity being reached or exceeded
- Location of access
- Severity of captured information

3 Policy Maintenance Responsibility

The Office of Administrative and Technology Services (OATS) IT Security & Audit Section is responsible for the maintenance of this policy.

4 Exceptions

Any exceptions to this policy must follow the procedures established in CHFS IT Policy: 070.203.

5 Policy Review Cycle

Annual

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS IT Policy: 040.101- Server/Application Backup and Retention Policy
- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- Internal Revenue Services (IRS) Publication 1075
- 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) Framework