



Information Technology (IT) Policy



065.004 New Application Development

Version 2.1
February 29, 2016



065.004 New Application Development	Current Version: 2.1
065.000 Application Development	Effective Date: 05/2/2005

Revision History

Date	Version	Description	Author
5/2/2005	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	

065.004 New Application Development	Current Version: 2.1
065.000 Application Development	Effective Date: 05/2/2005

Table of Contents

- 1 065.004 NEW APPLICATION DEVELOPMENT..... 4**
- 1.1 PURPOSE..... 4
- 1.2 SCOPE..... 4
- 1.3 ROLES AND RESPONSIBILITIES..... 4
 - 1.3.1 Security Lead..... 4
 - 1.3.2 Privacy Lead..... 4
 - 1.3.3 CHFS Staff..... 4
- 1.4 MANAGEMENT COMMITMENT..... 4
- 1.5 COORDINATION AMONG ORGANIZATIONAL ENTITIES..... 5
- 1.6 COMPLIANCE..... 5
- 2 POLICY REQUIREMENTS..... 5**
- 2.1 NEW APPLICATION DEVELOPMENT..... 5
 - 2.1.1 Step 1..... 5
 - 2.1.2 Step 2..... 5
 - 2.1.3 Step 3..... 5
 - 2.1.4 Step 4..... 5
- 3 POLICY MAINTENANCE RESPONSIBILITY..... 6**
- 4 EXCEPTIONS..... 6**
- 5 POLICY REVIEW CYCLE..... 6**
- 6 REFERENCES..... 6**



065.004 New Application Development	Current Version: 2.1
065.000 Application Development	Effective Date: 05/2/2005

1 065.004 New Application Development

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 application development policy. This document establishes the agency's New Application Development Policy which help manage risks and lays out guidelines for implementing security best practices with regards to developing a new application.

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 practice and commitments required. This role is responsible for the adherence of the New Application Development 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 New Application Development Policy alongside the Security Lead.

1.3.3 CHFS Staff

Responsible to adhere to the New Application Development Policy as well as referenced documents that pertain to the development of new 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.

065.004 New Application Development	Current Version: 2.1
065.000 Application Development	Effective Date: 05/2/2005

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 New Application Development

OATS requires all new application development efforts to be reviewed and analyzed. All new application development shall follow established IT standards. Enhancements to existing systems will follow the processes outlined in CHFS IT Policy: 065.014- Software Development Lifecycle.

SharePoint sites created by the Division of Systems Management (DSM) Family Services Management Branch (FSSMB) are not included in this policy, unless custom coding is required.

All new application development efforts must follow the outlined steps below:

2.1.1 Step 1

New application development must be submitted to the IT Technical Architecture group for Analysis and approval of the technical architecture of the solution.

Submissions must be in accordance with the OATS IT Standard 024.001 (<http://chfs.ky.gov/os/oats/itstandards.htm>).

2.1.2 Step 2

The customer must sign-off on the vision, scope, and optional functional requirements that are documented.

2.1.3 Step 3

The OATS Security office, or an approved contractor, must perform a security assessment on the new application.

2.1.4 Step 4

The new application must undergo user acceptance testing (UAT) and receive the approved agency sign off before it is deployed into production.

065.004 New Application Development	Current Version: 2.1
065.000 Application Development	Effective Date: 05/2/2005

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 Standard: 8100- Application Development Methodology & Software Standard
- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- CHFS IT Policy: 065.014- Software Development Lifecycle 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