



Information Technology (IT) Policy



065.016 Configuration Management

Version 2.1
February 9, 2016

065.016 Configuration Management	Current Version: 2.1
065.000 Application Environment	Effective Date: 12/16/2011

Revision History

Date	Version	Description	Author
12/16/2011	1.0	Effective Date	CHFS IT Policies Team Charter
2/9/2016	2.1	Revision Date	CHFS IT Policies Team Charter
2/9/2016	2.1	Review Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Executive Director (or designee)	2/9/2016	Bernard Decker	

065.016 Configuration Management	Current Version: 2.1
065.000 Application Environment	Effective Date: 12/16/2011

Table of Contents

- 1 065.016 CONFIGURATION MANAGEMENT4
 - 1.1 PURPOSE.....4
 - 1.2 SCOPE.....4
 - 1.3 ROLES AND RESPONSIBILITIES4
 - 1.3.1 Security Lead.....4
 - 1.3.2 Privacy Lead.....4
 - 1.3.3 CHFS Staff.....4
 - 1.4 MANAGEMENT COMMITMENT4
 - 1.5 COORDINATION AMONG ORGANIZATIONAL ENTITIES4
 - 1.6 COMPLIANCE.....5
- 2 POLICY REQUIREMENTS5
 - 2.1 CONFIGURATION MANAGEMENT5
 - 2.1.1 Baseline Configuration.....5
 - 2.1.2 Configuration Change Control.....5
 - 2.1.3 Configuration Settings.....5
- 3 POLICY MAINTENANCE RESPONSIBILITY5
- 4 EXCEPTIONS.....6
- 5 POLICY REVIEW CYCLE.....6
- 6 REFERENCES.....6

065.016 Configuration Management	Current Version: 2.1
065.000 Application Environment	Effective Date: 12/16/2011

1 065.016 Configuration Management

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 a configuration management policy. This document establishes the agency's Application Configuration Management Policy which help manage risks and lays out guidelines for implementing security best practices in regards to configuration management.

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

1.1.1 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 Configuration Management Policy.

1.1.2 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 Configuration Management Policy alongside the Security Lead.

1.1.3 CHFS Staff

Must adhere to the Configuration Management 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.

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet who access

065.016 Configuration Management	Current Version: 2.1
065.000 Application Environment	Effective Date: 12/16/2011

their applications or systems. All organizational entities that interact with OATS are subject to follow guidelines outline 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 Configuration Management

The CHFS agencies whom deal with Internal Revenue Services (IRS) Federal Tax Information (FTI) will follow the guidelines and regulations within the Publication 1075 for software applications configuration management needs.

2.1.1 Baseline Configuration

CHFS agencies follow the COT OIS-053 Windows Server Security Configuration Documentation Annual Review Process. This finalized process establishes the baseline security configuration for all windows systems supported by the COT windows Server Support Team.

2.1.1 Configuration Change Control

CHFS agencies follow the CHFS 010.103- Change Control Policy and CHFS 065.014- Division of Systems Management System Development Life Cycle Policy in regards to change control guidelines.

2.1.1 Configuration Settings

CHFS agencies will follow the COT security configuration guidelines, which include mandatory configurations of information systems, for a baseline for configuration settings. Any exceptions from these mandatory configurations must go through the formal approval process by following CHFS 070.203- Exceptions to Standards and Policies Policy.

3 Policy Maintenance Responsibility

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

065.016 Configuration Management	Current Version: 2.1
065.000 Application Environment	Effective Date: 12/16/2011

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: 010.103- Change Control Policy
- CHFS IT Policy: 065.014- Division of Systems Management System Development Life Cycle Policy
- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- Enterprise IT Process: OIS-053- Windows Server Security Configuration Documentation Annual Review Process
- 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