



Information Technology (IT) Policy



010.103 Change Control

Version 2.1
September 16, 2016

010.103 Change Control	Current Version: 2.1
010.000 Logical Security	Effective Date: 06/21/2007

Revision History

Date	Version	Description	Author
6/21/2007	1.0	Effective Date	CHFS IT Policies Team Charter
9/16/2016	2.1	Revision Date	CHFS IT Policies Team Charter
9/16/2016	2.1	Review Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	9/16/2016	Robert Pugh	

010.103 Change Control	Current Version: 2.1
010.000 Logical Security	Effective Date: 06/21/2007

Table of Contents

1	010.103 CHANGE CONTROL	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	GENERAL CHANGE CONTROL.....	5
2.2	DESCRIPTION OF COMPONENTS	5
2.3	CHANGE CONTROL PROCESS	6
2.3.1	<i>Production and Training Systems Environment</i>	6
2.3.2	<i>Development and Testing Systems Environment</i>	6
2.3.2.1	<i>Dedicated Environment</i>	6
2.3.2.2	<i>Shared Environment</i>	6
2.3.3	<i>Request Submission</i>	7
3	POLICY MAINTENANCE RESPONSIBILITY	8
4	EXCEPTIONS	8
5	POLICY REVIEW CYCLE	8
6	REFERENCES	8

010.103 Change Control	Current Version: 2.1
010.000 Logical Security	Effective Date: 06/21/2007

1 010.103 Change Control

Category: 010.000 Logical Security

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a change control policy. This document establishes the agency's Change Control Policy which helps manage risks and provides guidelines for security best practices regarding change control.

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. This policy does not cover the mainframe change control process. Please refer to CHFS 065.014 Division of Systems Management SDLC Policy for the mainframe change control process.

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 Change Control Policy.

1.3.2 Privacy Lead

Individual responsible for enforcing security and privacy guidance, of sensitive information, to all CHFS information technology (IT) personnel. This role is responsible for the adherence of the Change Control Policy alongside the Security Lead.

1.3.3 CHFS Staff

Must adhere to the Change Control 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 Chief Information Officer (CIO). Senior Management supports the objective put into place by this policy.

010.103 Change Control	Current Version: 2.1
010.000 Logical Security	Effective Date: 06/21/2007

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet which access applications or systems. All organizational entities that interact with CHFS systems are subject to follow requirements outlined within this policy.

1.6 Compliance

CHFS abides by the security and privacy requirements 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 General Change Control

The Change Control Policy was implemented to establish unified control for changes to all servers. The Change Control Board (CCB) was established to ensure that the Change Control Policy is implemented and maintained as published. All data fixes shall be logged and recorded by the appropriate agency, and shall be auditable. Any data fix that requires a database restart or system reboot, CCB approval must be obtained

2.2 Description of Components

CHFS IT has implemented a change control process consisting of, but not limited to, an online change control portal, a weekly meeting of a designated change control approval board, and an emergency approval contact list.

An online portal for the purpose of submitting, reviewing, and monitoring all change controlled processes has been established. The availability of this portal has been limited to technology personnel. The change control portal may be accessed via: <https://webapp.chfsinet.ky.gov/ITMP/home.aspx>.

The CCB carries the responsibility of managing all change control requests. This responsibility consists of the review, approval, denial and referral of such requests. The CCB shall consist of at least one representative of each affected branch within IT. The CCB shall meet weekly at a designated and published time (this can be by conference call.) The CCB does not possess the responsibility to verify the technical feasibility of requested changes. This responsibility falls on the requestor or requestor's designee. Nor does the CCB act in place of management approval. All requests must be planned and cleared by all normal internal processes before a change control request is submitted.

010.103 Change Control	Current Version: 2.1
010.000 Logical Security	Effective Date: 06/21/2007

The emergency approval designees hold the responsibility for approving all requests deemed an emergency. This shall consist of a primary and a secondary contact. There is an adequate assumption that such requests should receive a response within three (3) hours. In such times there has been no response to an emergency request within three hours, the request should be forwarded to the CCB Chairperson and/or upper level executive management.

2.3 Change Control Process

2.3.1 Production and Training Systems Environment

No change, including but not limited to; Hardware, Operating System, System Restarts and Application, shall be committed to a production system without the submission and prior approval of the standard Change Control Request process.

All CCB approved requests must then be submitted to the Commonwealth Office of Technology's (COT) Change Advisory Board (CAB) for final approval and action.

2.3.2 Development and Test Systems Environment

2.3.2.1 Dedicated Environments

A dedicated Development and Test Environments would have exclusive use of specific services provided on a server.

By definition, a dedicated environment could have functionally related applications, databases and report services.

All changes to non-production, except Development, (application modifications, database modifications, etc.) shall be entered into the ITMP change control portal for documentation purposes only. Lower environment change controls do not require CCB approval.

2.3.2.2 Shared Environments

A shared environment is any environment where non-related application, database, report, or other services for different application platforms (Development, Test, Training, and Production) are housed on the same server. Multiple applications hosted on the same server are also considered shared environments.

No change concerning any modification of hardware, operating systems, installation of new applications, databases (i.e. SQL, Oracle), or system restarts shall be committed to a non-production, shared system without the submission and prior approval of a change control request to the CCB.

010.103 Change Control	Current Version: 2.1
010.000 Logical Security	Effective Date: 06/21/2007

All other changes (application modifications, database modifications, etc.) shall be entered into the change control portal for documentation purposes only.

2.3.3 Request Submission

All testing, planning, notification and management approval must be completed prior to submitting a change control request. Upon submission, all requests must be completed as fully as possible. Failure to complete a required task, provide proper, adequate or required information may result in the denial or delay of the change request.

Change requests must be submitted in a timely manner. All non-emergency requests shall be reviewed weekly during the regularly scheduled change control meeting. All requests received after 10:00 am, the morning of the scheduled meeting, shall be reviewed during the following week's CCB meeting.

Careful evaluation needs to be supplied to the following areas when submitting a change control request:

Risk Factor Level	Risk Factor Description
Minimum	Little to no impact of current services
Medium	Clear and noticeable impact of services
Severe	Significant impact on the services and the business. Considerable manpower and/or resources needed.

Impact Level	Impact Description
Low	Change leads to minor improvement
Medium	Change will solve irritating errors or missing functionality
High	Change needed as soon as possible (Potentially damaging)
Emergency	Change necessary now (Otherwise severe business impact) *May not be applicable to scenarios that could have/should have been planned

Upon submittal of a change control request, the request shall be assigned to the next available change control meeting. During this time the CCB will review the request, verify scheduling and cross project impact. Once the CCB has made their decision, the requestor shall be notified.

Upon CCB approval of a change control request, the requestor may proceed with the change. If the scheduling and/or scope of the change varies from the approved request, then the change control will need to be postponed and resubmitted for approval.

010.103 Change Control	Current Version: 2.1
010.000 Logical Security	Effective Date: 06/21/2007

Upon denial of a change control request, all intended operations must be stopped. The requestor may view the change control request for comment from the CCB and resubmit accordingly.

If there is a change of status for any request, including completion of tasks, it is the requestor's responsibility to review and update the request.

Prior to CCB approval the requestor would submit their request to the Commonwealth Service Desk (CommonwealthServiceDesk@Ky.Gov) to open a ticket. The ticket is either for assistance or information, if a vendor is completing the release. If available, all requests must include documentation with release instructions.

3 Policy Maintenance Responsibility

The Office of Administrative and Technology Services (OATS) IT Security & Compliance Team 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

This policy is reviewed and/or revised on an as needed basis, but at least once annually.

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- 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 Procedure: CIO-067- COT Security Standard Procedure Manual (SSPM)
- Enterprise IT Procedure: CIO-009- Change Management Procedure
- 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