



Information Technology (IT) Policy



040.301 Business Continuity Planning

Version 1.0
September 16, 2016

040.301 Business Continuity Planning	Current Version: 1.0
040.000 Contingency Planning and Operations	Effective Date: 9/16/2016

Revision History

Date	Version	Description	Author
9/16/2016	1.0	Effective Date	CHFS IT Policies Team Charter
9/16/2016	1.0	Revision Date	CHFS IT Policies Team Charter
9/16/2016	1.0	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 Puth	

040.301 Business Continuity Planning	Current Version: 1.0
040.000 Contingency Planning and Operations	Effective Date: 9/16/2016

Table of Contents

1	040.301 BUSINESS CONTINUITY PLANNING	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>BCP Coordinator</i>	4
1.3.4	<i>Designated Agency Leads</i>	4
1.3.5	<i>Agency Staff</i>	4
1.4	MANAGEMENT COMMITMENT.....	5
1.5	COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.6	COMPLIANCE.....	5
2	POLICY REQUIREMENTS	5
2.1	BUSINESS CONTINUTIY PLAN (BCP)	5
2.2	BCP DOCUMENTATION REPOSITORY	6
3	POLICY MAINTENANCE RESPONSIBILITY	6
4	EXCEPTIONS.....	6
5	POLICY REVIEW CYCLE	6
6	REFERENCES	6

040.301 Business Continuity Planning	Current Version: 1.0
040.000 Contingency Planning and Operations	Effective Date: 9/16/2016

1 040.301 Business Continuity Planning

Category: 040.000 Contingency Planning / Operations

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish comprehensive methodology for business continuity through a Business Continuity Plan (BCP). The BCP methodology must outline the crucial steps for agencies to recover and resume business functions in the event of a situation that disrupts, or threatens to disrupt, agency business function (SSA, 2015, page 1). This document establishes the agency's BCP Policy and provides guidelines for security best practices regarding the establishment and implementation of a high level BCP framework.

1.2 Scope

Each CHFS agency is responsible for the establishment and implementation of an agency-specific BCP. The BCP must apply to all personnel, activities, and resources necessary to ensure the recovery and resumption of business function if normal operations are disrupted or threatened with disruption. Designated agency personnel must become familiar with the procedures and responsibilities within the BCP.

1.3 Roles and Responsibilities

1.3.1 Security Lead

The security lead is responsible for assessing, planning and implementing all required security standards. This role is responsible for adhering to the BCP.

1.3.2 Privacy Lead

The privacy lead is responsible for providing the security and privacy guidance of sensitive information to all CHFS information technology (IT) staff. This role is responsible for adhering to the BCP together with the Security Lead.

1.3.3 BCP Coordinator

An individual who helps regularly coordinate all BCP activities.

1.3.4 Designated Agency Leads

An organization or individual(s) within, or outside of, the agency that detects a situation or disruption and notifies appropriate parties. This position/role is a designated lead or group who is familiar with the BCP procedures.

1.3.5 Agency Staff

Agency staff must adhere to the BCP as well as referenced documents that pertain to business continuity.

040.301 Business Continuity Planning	Current Version: 1.0
040.000 Contingency Planning and Operations	Effective Date: 9/16/2016

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.

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 Business Continuity Plan (BCP)

BCP methodology must align with standards within NIST Special Publication 800-34 Revision 1. At a minimum, the following elements must be documented and addressed within the plan:

1. Listing of Business Functions
2. Business Continuity Team Organization Chart
3. Roles and Responsibilities
4. Emergency Readiness Plan
5. Plan Phases (includes steps from initial notification through reconstitution)
6. Listing of Interoperable Communications
7. Plan for Safeguarding of Sensitive Documentation (FTI, Vitals, etc.)
8. Awareness, Training, Testing and Exercises
9. Emergency Contact Lists, both internal and external
10. Alternate Site(s) Information
11. Recovery Team Information
12. Report Forms

040.301 Business Continuity Planning	Current Version: 1.0
040.000 Contingency Planning and Operations	Effective Date: 9/16/2016

2.2 BCP Documentation Repository

All agency BCPs and BCP templates must be uploaded and maintained on a specified OATS SharePoint collection site. Each agency is responsible for uploading, updating, and finalizing BCP documents. OATS will be responsible for the administering of the site, including the management of site membership. The agency's BCP Coordinator, Agency Leads, or designee, must keep a softcopy of the agency's BCP and templates for backup in case there is an incident or outage of the Cabinets SharePoint site.

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

- Business Continuity Plan (BCP) Template
- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- Internal Revenue Services (IRS) Publications 1075
- National institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information
- National institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National institute of Standards and Technology (NIST) Special Publication 800-12 An Introduction to Computer Security
- 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
- Social Security Administration (SSA)- 2015 Business Continuity Plan (BCP) for Disability Determination Services (DDS)