Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy

040.301 Business Continuity Plan (BCP) Policy

Version 1.7
December 1, 2023

Revision History

Date	Version	Description	Author
9/16/2016	1.0	Effective Date	CHFS IT Policies Team Charter
12/1/2023	1.7	Review Date	CHFS Policy Charter Team
12/1/2023	1.7	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	12/1/2023	Jeremy Rogers	DocuSigned by: Jeremy Rogers FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or designee)	12/1/2023	Kelvin Brooks	DocuSigned by: Kelvin Brooks A0C20CD57C0E4B6...

Table of Contents

1 Policy Definitions

- **Business Continuity Planning:** Defined by CHFS as the creation of a strategy through the recognition of threats and risks facing a company, ensuring that personnel and assets are protected and able to function in the event of a disaster.
- **Business Continuity Plan:** Defined by NIST 800-34 Revision 1 as documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes must sustain during and after a significant disruption.
- **Business Impact Analysis (BIA):** A process that identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on business operations.
- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law (Kentucky Revised Statute 61.878); Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e., System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Data Classification:**
    - **NIST High Impact Level:** Defined by NIST 800-53 Revision 4 as an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high; severe or catastrophic effect on organizational operations, organizational assets, or individuals resulting in severe degradation to or a complete loss of an organization's ability to carry out its mission, severe financial loss, and/or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
    - **NIST Moderate Impact Level:** Defined by NIST 800-53 Revision 4 as an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a FIPS Publication 199 potential impact value of high; serious adverse effect on organizational operations, organizational assets, or individuals including resulting in significant degradation to an organization's ability to carry out its mission, significant financial loss, and/or significant but non-life-threatening harm to individuals.
    - **NIST Low Impact Level:** Defined by NIST 800-53 Revision 4 as an information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low; limited adverse effect on organizational operations, organizational assets, or individuals resulting in minor degradation to an

organization’s ability to carry out its mission, minor financial loss, and/or minor harm to individuals.

- **Electronic Personal Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual’s past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Identifiable protected health information items include many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- **Enterprise Identity Management (EIM):** Defined by the Enterprise Identity Management User Guide as the Commonwealth Office of Technology’s (COT) solution for identity management for employees and other users in the Commonwealth. EIM is a centralized system designed to standardize account creation, modification, and removal for users in the Commonwealth. EIM manages Active Directory, Email, and Home Folder(s).
- **Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency’s possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.
- **Maximum Tolerable Downtime (MTD):** The maximum period of time that a given business process can be inoperative before the organization's survival is at risk.
- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61.931-934 and in accordance with NIST 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person’s first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account;

social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA). In addition, HIPAA identifies an individual's full name, date of birth, street or email address, biometric data, and other common identifiers as direct PII not requiring a combined additional field of information.

- **Recovery Point Objective (RPO):** Defined by NIST 800-34 Revision 1 as the point in time to which data must be recovered after an outage.
- **Recovery Time Objective (RTO):** Defined by NIST 800-34 Revision 1 as the overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.
- **Sensitive Data:** Defined by COT standards as is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: all information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information. The Commonwealth's proprietary information including but not limited to intellectual property, financial data and more.
- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS with final approval and appointment by the Kentucky Personnel Cabinet.
- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a 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(s). 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.

2.2 Scope

Each CHFS division is responsible for designing BCPs necessary to meet the policy purpose listed above. The BCP must apply to all personnel, activities, and resources necessary to ensure recovery and normal resumption of business function/operations are achieved after disrupted or threatened with disruption. Designated personnel shall be familiar with the procedures and responsibilities within the BCP.

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

CHFS organizations and/or agencies that access applications, systems, and facilities work in coordination to ensure requirements outlined in this policy are followed. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the NIST. Applicable agencies additionally follow security and privacy frameworks outlined within CMS, IRS, and SSA.

3 Policy Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

An individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct HIPAA risk assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach. This position is responsible for adherence to this policy.

3.3 Chief/Deputy Technical Officer (CTO)

This individual makes decisions related to a company's technology. This includes the integration and deployment of new technology, systems management, and the overseeing of technical operations personnel. The CTO also works with outside vendors to ensure they meet customer service expectations. This individual is responsible for adherence to this document.

3.4 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for the protection of Payment Card Industry (PCI), PII, ePHI, FTI and other financially sensitive information to all CHFS staff/personnel. This role along with the CHFS IS Team is responsible for adherence to this policy.

3.5 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS information system(s).

3.6 System Data Owner and System Data Administrators

Management/Lead who work with the application's development team to document components that are not included in the base server build and ensure functionality and backups are conducted in line with business needs. This individual(s) is responsible for working with enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

3.7 Business Continuity Plan Coordinator

Designated individual(s) who coordinates and assists in the BCP development, maintenance, testing, document, and reporting strategies in conjunction with individuals responsible for other related plans such as the Disaster Recovery Plan. The BCP documents a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

The BCP Coordinator considers risk assessments, business impact analyses, prior BCP and other related testing reports or documents to plan, conduct, and report the results of disaster exercises performed annually or subsequent to a significant system change that test the adequacy of the exist plan. Perform a BCP plan review at least annually review making updates as needed.

3.8 Designated Agency Leads/Division Points of Contact

Individual(s) within, or outside of, the division that detects a situation or distribution and notifies appropriate parties. This position/role is a dedicated lead or group who is familiar with and adhere to the agency's BCP Procedures. The Designated Agency Lead(s) ensures the sustainment and delivery of business continuity and documentation for their agency, including testing, training, exercises, and updating (contact) information on an as needed basis.

3.9 Business Impact Analysis (BIA) Sponsor

The BIA sponsor, the application owner, project manager or designee documents the technical information in the BIA process for the assigned application. Coordinates BIA activities with the application business owner to determine the sensitivity and critical business operations impacts of a disaster, accident, or emergency related to the assigned application or service within the BIA process.

Following the BCP testing, the BCP Coordinator will facilitate a review of the plan test results initiating corrective action, if needed. The BCP coordinator is responsible for producing an after-action report to improve existing processes, procedures, and policies. Personnel responsible for each application will be responsible for making BCP test results available to the CHFS business owner.

4 Policy Requirements

4.1 Business Continuity Plan (BCP)

BCP methodology must align with standards within the National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information and other federal compliance requirements.

The following elements shall be documented and addressed within the plan:

1. Business Functions List

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. Interoperable Communications List
7. Safeguarding of Sensitive Documentation (FTI, Vitals, etc.) Plan
8. Awareness, Training, Testing and Exercises
9. Internal and External Emergency Contact Lists
10. Alternate Site(s) Information
11. Recovery Team Information
12. Report Forms

A BCP is developed and maintained for each CHFS and vendor managed application to meet how an organization's mission/business processes will be sustained during and after a significant disruption. The plan must:

- Apply FIPS 199 security categorization (low, moderate, high) to an application to determine the appropriate security controls.
- Assign specific responsibilities to designated staff to facilitate the recovery and/or continuity of essential system functions.
- Acquire and allocate resources necessary to ensure viability of the BCP.
- Train responsible application personnel to execute contingency testing and recovery procedures.
- Test contingency and recovery capabilities annually or subsequent to a significant system change using functional exercises determining the plan effectiveness readiness to execute.

4.2 BCP Documentation Repository

Each agency is responsible for uploading, updating, and finalizing BCP documents and templates to an agency designated secured repository. CHFS is responsible for the site administration, 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 at a designated off-site location for backup in case of an incident or outage of the CHFS SharePoint site.

4.3 Business Impact Analysis (BIA)

The BIA Sponsor for each application listed in the CHFS Application Inventory of the Information Technology Management Portal (ITMP) must, in coordination with the application business owner, create a BIA using the OATS BIA Site. The BIA will be used by the BCP Coordinator to characterize the system components, supported mission/business processes, and interdependencies. The BCP Coordinator will use the BIA results to document contingency planning requirements and priorities. The BIA for each application must be performed during the Initiation phase of the SDLC. The BIA includes a determination of the Maximum Tolerable Downtime (MTD), Recovery Point Objective (RPO), and Recovery Time Objective (RTO).

4.4 Preventive Controls Inventory

The BCP must include a list of existing preventive controls consisting of measures taken to reduce the effects of system disruptions, increase system availability, and reduce contingency life cycle costs. CHFS baseline preventive controls are NIST 800-53 moderate controls for all applications unless the application owner determines more stringent controls are required.

4.5 Contingency Strategies

The BCP must include strategies to mitigate the risk arising from use of information and information systems in the execution of mission/business processes. These strategies should be guided by the NIST Risk Management Framework and in accordance with FIPS 199 and NIST SP 800-53 Revision 4. Contingency strategies must cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance.

4.6 Disaster Recovery Plan (DRP)

The Disaster Recovery (DR) Coordinator or designated individual must develop and maintain a DRP that contains detailed guidance and procedures for restoring damaged systems unique their security impact level and recovery requirements identified in each system’s BIA. The DR Coordinator is responsible for the conducting of annual plan testing, training, and exercises to validate recovery capabilities meet the Maximum Tolerable Downtime (MTD), Recovery Point Objective (RPO), and Recovery Time Objective (RTO) objectives. The DR Coordinator is also responsible for annual plan maintenance and review to ensure that it remains current with ongoing system enhancements and organizational changes.

5 Policy Maintenance Responsibility

The CHFS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy.

7 Policy Review Cycle

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

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.2
- CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and

Security Control Policy

- Internal Revenue Services (IRS) Publication 1075
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- 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 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information