Commonwealth of Kentucky
Cabinet for Health and Family Services

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

040.101 Application Backup Policy

Version 2.3
December 3, 2020

Revision History

Date	Version	Description	Author
12/13/2006	1.0	Effective Date	CHFS IT Policies Team Charter
12/3/2020	2.3	Review Date	CHFS OATS Policy Charter Team
12/3/2020	2.3	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive Director (or designee)	12/3/2020	Jennifer Harp	DocuSigned by: Jennifer Harp 057B913AA3E14AE...
CHFS Chief Information Security Officer (or designee)	11/25/2020	Nicholas Tomlin	DocuSigned by: 55B6A12812DD403...

Table of Contents

1 Policy Definitions

- **Availability:** Defined by National Institute of Standards and Technology (NIST) 800-53 Revision 4 as ensuring timely and reliable access to and use of information.
- **Confidentiality:** Defined by NIST 800-53 Revision 4 as a preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **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 Protected 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.

- **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.
- **Integrity:** Defined by NIST 800-53 as the guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Mission Critical:** Defined by CHFS as any production applications developed, maintained or utilized by OATS that have a recovery time objective (RTO) of 7 days or less, a recovery point objective (RPO) based on the backup requirements that are typically nightly or otherwise specified, and/or federally mandated/regulated as critical. These applications are included in the Service Level Agreement (SLA) with COT as "Agency Critical Applications". These applications require creation and maintenance of Business Continuity Plan (BCP) which includes Business Impact Analysis (BIA) and Disaster Recovery Plan (DRP) documents.

  CHFS utilizes the NIST federal standards as well as FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems for determining its critical systems. Utilizing FIPS 199, a system is defined as critical when the potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- **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).

- **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 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 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.
- **System/Data Administrator:** Defined by CHFS as an individual who is responsible for the data administration process by which data is monitored, maintained, and managed. This person is responsible for controlling application data assets, as well as their processing and interactions with different applications and business processes. This person is also tasked with access management to the system/data using the Role-based Access Control (R-BAC) model. In the Cabinet for Health and Family Services this role is generally played by a CHFS Branch Manager.

- **System/Data Custodian:** Defined by CHFS as an individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department, which owns the Infrastructure. The duties include performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the enterprise security policies, standards, and guidelines that pertain to information security and data protection. In the Commonwealth of Kentucky this role is generally played by Commonwealth Office of Technology (COT).
- **System/Data Owner:** Defined by CHFS as the person who has final agency responsibility of data protection and is the person held liable for any negligence when it comes to protecting the specific application's data/information assets. This role/person is the owner of the system that holds the data, usually a senior executive, designates the confidentiality of the system/data, and assigns the data admin, and dictates how the information should be protected based on business' policies. In the Cabinet for Health and Family Services this role is generally played by a CHFS Business Executive.
- **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) Office of Application Technology Services (OATS) must establish a comprehensive level of security controls through an application backup policy. This document establishes the agency's Application Backup Policy that helps manage risks and provides guidelines for security best practices regarding system backups. To minimize the possible disruption to business operations, CHFS shall establish and maintain an effective schedule for the backup of critical data.

2.2 Scope

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

OATS 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

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. 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 the CMS, the IRS, and SSA.

3 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 Health Insurance Portability and Accountability Act (HIPAA) risk assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS 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 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 protection of PCI, PII, ePHI, FTI and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 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/OATS information system(s).

3.5 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) will be responsible to work 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.

4 Policy Requirements

4.1 Data Backup

All information technology systems in CHFS containing mission critical data are required to be backed-up on a regularly-scheduled basis and are replicated to an alternate data center location for continued operation of critical functions.

CHFS data and backups that have regulatory or compliance requirements, containing ePHI/PHI/PII/HIPAA/FTI/SSA/Sensitive data, shall be encrypted in transit and at rest. CHFS agencies that seek exception(s) to encryption of data and backups in transit or at

rest must follow guidance and obtain approval established in the CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy. Data at rest includes data stored in databases, backup archive files, file folders, file systems, and on removable media. Backups shall never leave the United States. Cloud or other storage must be scrutinized to ensure vendors are not storing CHFS data in a physical location outside of the U.S.; refer to CHFS 020.301 CHFS Network User Accounts Policy.

Upon request from the System Data Owner and/or the System Data Administrator, COT is responsible for performing application/data backups, on CHFS-hosted appliances. Vendors are responsible for application/data backups on non CHFS-hosted appliances. COT and vendors shall be responsible for the following:

a. Providing adequate operational resources for data backup and testing of media.
b. Instructing appropriate staff on data backup and recovery procedures.
c. Ensuring that application/data backup and recovery procedures are followed.
d. Ensuring that only authorized people with sufficient knowledge conduct the backup and recovery processes.
e. Ensuring compliance with all state and federal regulations during the backup and recovery processes.

The CHFS agency System Data Owner and/or the System Data Administrator is responsible for the backup, archival, and retention of paper documents (i.e., files, records, etc.). The CHFS agency shall follow applicable federal and state laws, regulations, and guidelines when handling paper archival documents.

4.1.1 Data to be Backed-up

All data needed to return an inoperable application to a normal state shall be backed up. By default, COT only backs up operating system files. The System Data Owner and/or the System Data Administrator must request COT to back up specific data. Examples include, but are not limited to, the following:

- All configuration settings applicable to an application's functionality.
- All data deemed critical as defined by application owners.
- All applications' user accounts or key information related to accessing the application.

4.2 Backup Frequency

Backup frequency is critical to successful data recovery. In determining the backup frequency, the System Data Owner and/or the System Data Administrator must determine the Recovery Point Objective (RPO).

4.3 Backup Storage

Data/Application backups typically contain confidential information and, as such, precaution must be taken to ensure the security and integrity of the data and the medium on which that data resides. On-site and off-site storage must be in a secure,

access-controlled area and must use accepted methods of environmental controls to include fire suppression.

4.4 Backup Retention

Backup and retention schedules are based on the criticality of the data being processed and the frequency in which that data is modified. The System Data Owner and/or the System Data Administrator is/are responsible for working with COT for file and log backup retention schedules to meet necessary business requirements, NIST 800-53 Revision 4 compliance, CHFS Records Retention Schedule, Kentucky Department for Libraries and Archives (KDLA), as well as applicable federal and state regulations.

4.5 Backup Restoration Procedures and Testing

The System Data Owner and/or the System Data Administrator shall have restoration procedures documented and tested. Documentation must include, but is not limited to, the following:

- Responsible party to approve a restore;
- Process followed to restore;
- Under what circumstances it is to be performed;
- Time required from request to restoration; and
- Defined acceptable Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Backup restoration testing, (i.e. full application functionality test, smoke testing, operations readiness and assurance testing, etc.) must be performed at least one (1) time per year and additionally when any change is made that may affect the backup system(s). Results of the restoration tests shall be documented by the System Data Owner and/or the System Data Administrator and available upon request.

Although the agencies System Data Owner(s) are responsible for defining the duration of onsite versus offsite storage, restoration documentation and test results must be retained for at least ten (10) years in accordance with the CHFS Records Retention Schedule, Kentucky Department for Libraries and Archives (KDLA) requirements.

5 Policy Maintenance Responsibility

The OATS 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 OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS 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 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS Records Retention Schedule, Kentucky Department for Libraries and Archives (KDLA)
- Enterprise IT Policy: CIO-058 IT Equipment Room Access at the Commonwealth Data Center Policy
- Enterprise IT Policy: CIO-059 Equipment Installation and Removal at the Commonwealth Data Center Policy
- Enterprise IT Procedure: COT-009- Change Management Procedure
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems
- 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