

Commonwealth of Kentucky

Cabinet for Health and Family Services



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



070.501 CHFS Supply Chain Risk Management (SCRM) Policy

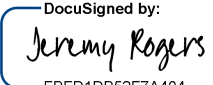

**Version 1.0
April 2, 2025**

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

Revision History

Date	Version	Description	Author
04/02/2025	1.0	Effective Date	CHFS IT Policies Team Charter
04/02/2025	1.0	Review Date	CHFS IT Policies Team Charter
04/02/2025	1.0	Revision Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	4/3/2025	Jeremy Rogers	DocuSigned by:  FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or delegate)	4/2/2025	kelvin Brooks	Signed by:  A0F3F24DC182406...

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

Table of Contents

- 1. POLICY DEFINITIONS 5
- 2. POLICY OVERVIEW 6
 - 2.1. Purpose 6
 - 2.2. Scope 6
 - 2.3. Management Commitment..... 6
 - 2.4. Coordination among Organizational Entities 6
 - 2.5. Compliance..... 6
- 3. ROLES AND RESPONSIBILITIES 6
 - 3.1. Chief Information Security Officer (CISO)..... 6
 - 3.2. Chief Privacy Officer (CPO) 6
 - 3.3. CHFS Information Security (IS) Team 7
 - 3.4. Chief/ Deputy Chief Technology Officer (CTO) 7
 - 3.5. Security/Privacy Lead 7
 - 3.6. CHFS Contract, State, and Vendor Staff/Personnel 7
 - 3.7. Supply Chain Chief Risk Officer 7
 - 3.8. Supply Chain Risk Manager..... 7
 - 3.9. Supplier Relationship Manager 7
 - 3.10. Supply Chain Risk Analyst..... 8
 - 3.11. Supply Chain Compliance Officer 8
 - 3.12. COT Kentucky Information Technology Standards (KITS) Coordinator 8
- 4. POLICY REQUIREMENTS 8
 - 4.1. Supply Chain Risk Management Plan 8
 - 4.2. Supply Chain Risk Management Team 8
 - 4.3. Supply Chain Risk Identification and Assessment..... 9
 - 4.4. Supply Chain Risk Mitigation and Controls 9
 - 4.5. Supplier Assessment and Reviews 9
 - 4.6. Notification Agreements 9
 - 4.7. Component Inspection 10
 - 4.8. Component Authenticity 10
 - 4.9. Component Disposal..... 10
- 5. POLICY MAINTENANCE RESPONSIBILITY 10
- 6. POLICY EXCEPTIONS 10

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

7. POLICY REVIEW CYCLE 10

8. POLICY REFERENCES 10

9. Control Mapping..... 11



070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

1. POLICY DEFINITIONS

- **Asset:** An asset can be any CHFS-owned systems, servers, network devices, software and applications.
- **Contract:** A legally binding agreement between CHFS and Third-Parties outlining information security terms and conditions. The agreement could be documented by a formal contract, memorandum of agreement, memorandum of understanding, statement of work, and/or invoice (for less material engagements).
- **Due Diligence:** Research and information security analysis of a company or organization done in preparation for a business transaction (such as a corporate merger or purchase of securities).
- **Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- **Risk:** Defined by NIST SP 800-30 as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information System security related risk is one that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation.
- **Risk Assessment:** Defined by NIST SP 800-30 as the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
- **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.
- **Threat:** Defined by NIST SP 800-30 as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
- **Third-Party Provider:** Defined by CHFS as any contracted or government organization that is not a part of the agency’s organizational structure. This may include state or federal auditing agencies, state approved security contract vendors or other external organizations that provides products and/or services to CHFS.
- **Vendor Staff/Personnel:** Defined by CHFS as supplemental resources contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

2. POLICY OVERVIEW

2.1. Purpose

The Cabinet for Health and Family Services (CHFS) Supply Chain Risk Management (SCRM) Policy establishes a comprehensive level of security controls to manage supply chain risks. This document defines the security controls and provides guidelines for security best practices regarding supply chain risks, assessment of third-party providers and disposal of components.

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

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 coordinates with organizations and/or agencies within 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 National Institute of Standards and Technology (NIST). In addition, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare & Medicaid Services (CMS), Internal Revenue Services (IRS), and Social Security Administration (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

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

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. CHFS Information Security (IS) Team

The CHFS IS Team is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required.

3.4. Chief/ Deputy Chief Technology 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 third-party providers to ensure they meet customer service expectations. This individual is responsible for adherence to this document.

3.5. Security/Privacy Lead

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

3.6. 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).

3.7. Supply Chain Chief Risk Officer

An individual responsible to oversee the development and implementation of supply chain risk management strategies and ensure alignment of supply chain risk management with overall business objectives. This individual is responsible for adherence to this policy. CHFS CISO is responsible for this role.

3.8. Supply Chain Risk Manager

Individuals responsible to oversee the supply chain risk assessment activities, review the findings and risk ratings and monitor supply chain operations for risk indicators. This role has shared responsibilities. CHFS Office of Application Technology Services (OATS) IT Audit and Compliance Manager and Security Operations Manager are responsible for managing supply chain risks of third-party providers of commercial off-the-shelf (COTS) products and third-party providers of services (in consultation with Division of Procurement and Grant Oversight [DPGO] office) to CHFS.

3.9. Supplier Relationship Manager

Individuals responsible to manage the relationships with CHFS third-party providers to ensure compliance with risk management practices, collaborate with third-party providers to develop

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

risk mitigation plans, and negotiate contracts with risk management clauses. This role has shared responsibilities. Product Requestor and CHFS OATS Security Manager Special Projects is responsible for managing supply chain risks of third-party providers of COTS products and third-party providers of services (in consultation with DPGO office) to CHFS.

3.10. Supply Chain Risk Analyst

Individuals responsible to conduct the supply chain risk assessment of third-party providers, analyze their responses to identify potential supply chain risks, prepare risk assessment reports and collaborate with Supplier Relationship Manager and third-party provider in developing mitigation strategies. This role has shared responsibilities. CHFS OATS IEES POA&M Coordinator and Security Architect are responsible for managing supply chain risks of third-party providers of COTS products and third-party providers of services (in consultation with DPGO office) to CHFS.

3.11. Supply Chain Compliance Officer

An individual responsible to ensure supply chain operations comply with relevant regulations and standards, communicate supply chain risk policies and processes to stakeholders and monitor regulatory changes. CHFS OATS Information Security Analyst is responsible for this role.

3.12. COT Kentucky Information Technology Standards (KITS) Coordinator

An individual responsible to oversee and manage the products in KITS Library. This role acts as the final approver in adding the requested product to the library and reviewing the library every two years.

4. POLICY REQUIREMENTS

This section outlines the policy requirements related to supply chain risks and follows the order in which controls are presented in IRS Publication 1075 (November 2021) and CMS ARC-AMPE (March 2025). Section 9 of this document provides the mapping of the policy requirements to applicable controls.

4.1. Supply Chain Risk Management Plan

CHFS agencies follow the <CHFS Supply Chain Risk Management (SCRM) Plan> that defines information security requirements for identifying and managing supply chain risks associated with the third-party provider throughout the engagement lifecycle (i.e., planning, due diligence, contracting, monitoring, and termination). The plan includes but not limited to the following:

- a process for the identification of supply chain risks
- acceptable supply chain risk mitigation strategies or controls
- a process for consistently evaluating and monitoring supply chain risk
- roles and responsibilities associated with maintenance of the plan

4.2. Supply Chain Risk Management Team

CHFS established a Supply Chain Risk Management Team (SCRMT) that oversees the evaluation, revision, creation, and maintenance of supply chain processes. The team consists of appropriate personnel with roles sufficient to lead and support SCRM functions.

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

The SCRMT includes representatives from various functional areas such as CHFS OATS Security & Compliance, DPGO office and Commonwealth Office of Technology (COT) to ensure a comprehensive approach to managing supply chain risks. The roles and responsibilities of the SCRMT are detailed in section 3, “Roles and Responsibilities”, of this document and in the <CHFS Supply Chain Risk Management (SCRM) Plan>.

4.3. Supply Chain Risk Identification and Assessment

CHFS identifies supply chain risks as part of the due diligence and continuous monitoring processes detailed in the Supply Chain Risk Management Plan. CHFS performs an assessment of the third-party provider prior to onboarding and annually thereafter to validate security control implementation, operations, and outcomes as per contractual requirements. The assessment process of third-party providers is detailed in the CHFS Supply Chain Risk Management (SCRM) Procedure.

4.4. Supply Chain Risk Mitigation and Controls

CHFS requires third-party providers to employ acceptable security controls through the requirements in contracts and agreements. The third-party providers are required to adhere to supply chain controls mentioned in [Office of the Chief Information Officer Enterprise Controls ENT-201: Enterprise Security Controls and Best Practices](#).

CHFS has clauses in place in the Master Agreements that require provisions and requirements for third-party providers flow down to any subcontractors. The subcontractors, if leveraged, are contractually obligated to adhere to the same agreements as those of the third-party provider as well as the [CHFS Business Associates and Third-Party Agreements Policy](#) as needed.

4.5. Supplier Assessment and Reviews

CHFS performs an annual assessment of its third-party providers in the Enterprise Governance Risk and Compliance (eGRC) system to understand their security posture. The annual assessment process of third-party providers is detailed in the CHFS Supply Chain Risk Management (SCRM) Procedure.

4.6. Notification Agreements

CHFS has developed the CHFS Notification and Continuous Monitoring of Outsourced Information System Procedure for formulating the requirement of documenting service level agreements (SLAs) to define expectations of performance, describing measurable outcomes, and identifying remedies and response requirements for any identified instance of non-compliance.

CHFS and its third-party providers follow the [Information Systems Incident Response and Reporting](#) and [CHFS OATS Incident Response Plan](#), which help to address the following:

- Incident Response: Containing, mitigating, and resolving incidents and/or breaches of data, including security and privacy incidents.
- Breach Notification: Defining the coordination among various organizational and non-organization entities, including all regulatory requirements regarding the investigation, management, and reporting of suspected or actual information security incidents, and/or security breaches.



070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

Additionally, CHFS requires the third-party providers to provide applicable regulatory authorization and compliance certifications that demonstrate their security posture prior to onboarding them. Post onboarding, CHFS conducts an annual assessment of third-party providers in Archer system and notifies the results to third-party providers. The assessment process third-party providers are detailed in the <CHFS SCRM Procedure>.

4.7. Component Inspection

CHFS agencies follows the <CHFS Anti-counterfeit Policy> for component inspection.

4.8. Component Authenticity

CHFS agencies follows the <CHFS Anti-counterfeit Policy> for component authenticity.

4.9. Component Disposal

CHFS agencies follow the [CIO-092 Media Protection Policy](#) and [CIO-102: Technology Sunset Policy](#) for secure disposal of data, documentation, tools, technology and system components.

5. POLICY MAINTENANCE RESPONSIBILITY

The CHFS IS Team is responsible for the maintenance of this policy. The policy is stored in CHFS controlled SharePoint and access is restricted to CHFS authorized personnel.

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 annually and revised on an as needed basis.

8. POLICY REFERENCES

- [CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy](#)
- CHFS Notification and Continuous Monitoring of Outsource Information System Services Procedure
- [CHFS Business Associates and Third-Party Agreements Policy](#)
- [Enterprise IT Policy CIO-092 Media Protection Policy](#)
- [Enterprise IT Policy CIO-102: Technology Sunset Policy](#)
- [CHFS Information Systems Incident Response and Reporting](#)
- [CHFS OATS Incident Response Plan](#)
- CHFS Anti-counterfeit Policy
- CHFS Supply Chain Risk Management (SCRM) Plan
- CHFS Supply Chain Risk Management (SCRM) Procedure
- [Office of the Chief Information Officer Enterprise Controls ENT-201: Enterprise Security Controls and Best Practices](#)
- Internal Revenue Services (IRS) Publications 1075 (2021)
- CMS ARC-AMPE_Vol2_SSPP-ACA-AE (March 2025)
- [National Institute of Standards and Technology \(NIST\) Special Publication 800-53 Revision 5 \(12/10/2020\)](#)

070.501 Supply Chain Risk Management Policy	Current Version: 1.0
070.000 Administrative	Review Date: 04/02/2025

- [National Institute of Standards and Technology \(NIST\) Special Publication 800-30 Revision 1 \(September 2012\)](#)

9. Control Mapping

The Supply Chain Risk (SR) controls from IRS Publication 1075 (November 2021) and CMS Acceptable Risk Controls for ACA, Medicaid and Partner Entities (ARC-AMPE) (March 2025) were used in drafting the policy requirements in section 4. The below table provides the control mapping to policy requirements.

Section	IRS Publication 1075 (November 2021)	ARC-AMPE (March 2025)	NIST 800-53 Rev5 (September 2020)*
4.1. Supply Chain Risk Management Plan	SR-2	SR-2	SR-2
4.2. Supply Chain Risk Management Team	SR-2(1)	SR-2(1)	SR-2(1)
4.3. Supply Chain Risk Identification and Assessment	SR-3	SR-3	SR-3
4.4. Supply Chain Risk Mitigation and Controls	SR-3, SR-3(2), SR-3(3)	SR-3	SR-3, SR-3(2), SR-3(3)
4.5. Supplier Assessment and Reviews	SR-6		SR-6
4.6. Notification Agreements		SR-8	SR-8
4.7. Component Inspection	SR-10		SR-10
4.8. Component Authenticity	SR-11, SR-11(1), SR-11(2)		SR-11, SR-11(1), SR-11(2)
4.9. Component Disposal		SR-12	SR-12

* Supply Chain Risk control requirements listed in the NIST 800-53 Rev5 column above are limited to the control requirements that are in IRS Publication 1075 and CMS ARC-AMPE.