

Commonwealth of Kentucky

Cabinet for Health and Family Services



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



070.601 CHFS Anti-Counterfeit Policy



**Version 1.0
July 17, 2025**

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

Revision History

Date	Version	Description	Author
07/17/2025	1.0	Effective Date	CHFS IT Policies Team Charter
07/17/2025	1.0	Review Date	CHFS IT Policies Team Charter
07/16/2025	1.0	Revision Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	7/17/2025	Jeremy Rogers	DocuSigned by:  FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or delegate)	7/16/2025	Kelvin Brooks	Signed by:  A0F3F24DC182406...

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

Table of Contents

1. POLICY DEFINITIONS	4
2. POLICY OVERVIEW	5
2.1. Purpose	5
2.2. Scope	5
2.3. Management Commitment	5
2.4. Coordination among Organizational Entities	5
2.5. Compliance	5
3. ROLES AND RESPONSIBILITIES	5
3.1. CHFS Chief Information Security Officer (CISO)	5
3.2. CHFS Chief Privacy Officer (CPO)	5
3.3. CHFS Information Security (IS) Team	6
3.4. Chief/ Deputy Chief Technology Officer (CTO)	6
3.5. Security/Privacy Lead	6
3.6. CHFS Contract, State, and Vendor Staff/Personnel	6
3.7. COT Asset Management Branch (AMB)	6
3.8. COT Monitoring and Response Branch	6
3.9. COT Kentucky Information Technology Standards (KITS) Coordinator	7
4. POLICY REQUIREMENTS	7
4.1. Procurement and Third-Party Provider Management	7
4.2. Training and Awareness	7
4.3. Detection and Verification	8
4.3.1. Inspection of Components	8
4.3.2. Verification Methods	8
4.3.3. Maintenance and Repair	8
4.4. Handling Suspected or Confirmed Counterfeit Components	8
5. POLICY MAINTENANCE RESPONSIBILITY	8
6. POLICY EXCEPTIONS	8
7. POLICY REVIEW CYCLE	8
8. POLICY REFERENCES	9
9. Control Mapping	9

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

1. POLICY DEFINITIONS

- **Asset:** An asset can be any CHFS-owned software and applications and/or any COT-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.
- **Counterfeit:** An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source.
- **Tampering:** An intentional, unauthorized act that leads to changes in a system, its components, its intended functionality, or the data it processes.
- **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.

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

2. POLICY OVERVIEW

2.1. Purpose

The Cabinet for Health and Family Services (CHFS) Anti-Counterfeit Policy establishes well-defined mechanisms aimed at preventing, detecting, and reporting counterfeit components within the IT supply chain, ensuring the integrity and security of the systems. This document defines the security controls and provides guidelines for security best practices regarding component inspection and component authenticity.

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. CHFS 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. CHFS 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

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

will conduct Health Insurance Portability and Accountability Act (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. 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. COT Asset Management Branch (AMB)

The Commonwealth Office of Technology (COT) Asset Management Branch is responsible to oversee and manage the hardware and software asset management processes for the Executive Branch of State Government which includes CHFS agencies. This team conducts inspection of components and detection of counterfeit components in the CHFS IT environment. Additionally, this team provides oversight and assistance in maintaining asset information in ServiceNow.

3.8. COT Monitoring and Response Branch

The Monitoring and Response Branch is responsible to provide 24-hour per day monitoring of enterprise sources, infrastructure stability monitoring, security incident monitoring, enterprise security incident management, enterprise risk and security architecture and infrastructure management.

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

3.9. COT Kentucky Information Technology Standards (KITS) Coordinator

An individual responsible for overseeing and managing the products in the 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 the management of counterfeit components. Section 9 of this document provides the mapping of the policy requirements to applicable controls in IRS Publication 1075 (November 2021).

4.1. Procurement and Third-Party Provider Management

A robust procurement process and well-defined third-party provider management effectively mitigates the risk of counterfeit components entering the system and ensures the integrity and reliability of products.

CHFS agencies follow the [CHFS Supply Chain Risk Management \(SCRM\) Policy](#), [CHFS Supply Chain Risk Management \(SCRM\) Plan](#), and the [CHFS Supply Chain Risk Management \(SCRM\) Procedure](#) for third-party provider risk management.

CHFS agencies have a centralized procurement process in place and follow the [070.110 Technology Acquisition Policy](#) for procurement of IT Hardware, Software, and Licenses.

CHFS agencies procure only from authorized and reputable third-party providers who can provide verifiable documentation of their products' authenticity.

CHFS maintains the list of third-party providers of commercial off-the-shelf (COTS) products and services in the eGRC system.

COT has defined Kentucky Information Technology Standards (KITS), which reflect a set of principles for information, technology, applications, and organization. These standards provide guidelines, policies, directional statements, and sets of standards for information technology. It defines, for the Commonwealth, functional and information needs so that technology choices can be made based on business objectives and service delivery. COT follows the [CIO-051: Information Technology Standards](#) for the development and maintenance of KITS. The [KITS Library](#) is reviewed by the KITS Coordinator every two years for currency.

4.2. Training and Awareness

COT provides training on the detection of counterfeit components (including hardware, software, and firmware) as part of the annual security and privacy awareness training to their staff. Additionally, knowledge transfer sessions are conducted for specific roles in the detection of counterfeit components. CHFS provides general guidance related to detecting and reporting counterfeit components as part of annual security and privacy awareness training for the State Staff/Personnel.

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

4.3. Detection and Verification

CHFS and COT Monitoring and Response Branch implements an Endpoint Detection and Response capability tool that employs defenses against the execution of potentially harmful software through behavioral, signature and heuristic detections.

Additionally, COT Asset Management Branch, in partnership with other COT Divisions and COT Monitoring and Response Branch, as applicable, perform the following for detection of counterfeit components:

- 4.3.1. **Inspection of Components-** Conducts thorough visual inspections of all incoming tangible products to verify their authenticity and identify any signs of tampering. Inspections include validating the ownership of the product, the presence of unique serial numbers or barcodes on the product, appropriate security labels, BitLocker encryption for hard drives etc.
- 4.3.2. **Verification Methods-** Conducts verification of software components through methods such as using File Integrity Monitoring solution to check for unauthorized modifications, downloading software from verified manufacturer websites.
- 4.3.3. **Maintenance and Repair:** Schedules, documents, and reviews records of maintenance, repairs, and replacement on system components in accordance with manufacturer or vendor specifications and COT requirements. The maintenance activities are authorized, logged, monitored, and controlled to prevent counterfeit components from entering the system. CHFS agencies follow the [CIO-114 - System Maintenance Policy](#), [CIO-092 Media Protection Policy](#), and [020.210 CHFS Non-Local Maintenance Policy](#) for configuration control over the system components awaiting service or repair and serviced or repaired components awaiting return to service.

4.4. Handling Suspected or Confirmed Counterfeit Components

CHFS follows the [CHFS Information Systems Incident Response and Reporting](#) and [CHFS OATS Incident Response Plan](#) for reporting and handling of counterfeit components.

COT follows the [CIO-090 - Information Security Incident Response Policy](#) and COT Incident Response Plan for reporting and handling of counterfeit components.

Per [ENT-201: Enterprise Security Controls and Best Practices](#), SR-11, detection of counterfeit components are reported internally to COT Office of the CISO.

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.

070.601 Anti-Counterfeit Policy	Current Version: 1.0
070.601 Contingency Planning/Operations	Review Date: 07/17/2025

8. POLICY REFERENCES

- [CHFS Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy](#)
- [070.110 Technology Acquisition Policy](#)
- [KITS Library](#)
- [CHFS Information Systems Incident Response and Reporting](#)
- [CHFS OATS Incident Response Plan](#)
- [CHFS Supply Chain Risk Management \(SCRM\) Policy](#)
- [CHFS Supply Chain Risk Management \(SCRM\) Plan](#)
- [CHFS Supply Chain Risk Management \(SCRM\) Procedure](#)
- [Internal Revenue Services \(IRS\) Publications 1075 \(2021\)](#)
- [CIO-051: Information Technology Standards](#)
- [CIO-090 - Information Security Incident Response Policy](#)
- [CIO-092 Media Protection Policy](#)
- [CIO-114 - System Maintenance Policy](#)
- [020.210 CHFS Non-Local Maintenance Policy](#)
- [ENT-201: Enterprise Security Controls and Best Practices](#)
- [National Institute of Standards and Technology \(NIST\) Special Publication 800-53 Revision 5 \(12/10/2020\)](#)
- [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) 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)	NIST 800-53 Rev5 (September 2020)*
4.1. Procurement and Third-Party Provider Management	SR-11	SR-11
4.2. Training and Awareness	SR-11(1)	SR-11(1)
4.3. Detection and Verification	SR-10, SR-11(2)	SR-10, SR-11(2)
4.4. Handling Counterfeit Components	SR-11	SR-11

* 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.