Commonwealth of Kentucky
Cabinet for Health and Family Services

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

KENTUCKY
CABINET FOR HEALTH
AND FAMILY SERVICES

020.210 CHFS Non-Local Maintenance Policy

Version 1.2
September 22, 2021

Revision History

Date	Version	Description	Author
10/29/2019	1.0	Effective Date	CHFS OATS Policy Charter Team
9/22/2021	1.2	Review Date	CHFS OATS Policy Charter Team
9/22/2021	1.2	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or designee)	9/22/2021	Jennifer Harp	DocuSigned by: Jennifer Harp 057B913AA3E14AE...
CHFS Chief Information Security Officer (or designee)	9/22/2021	Nicholas Tomlin	DocuSigned by: 55B6A12812DD403...

Table of Contents

1 POLICY DEFINITIONS 4

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 CHFS ROLES AND RESPONSIBILITIES 7

3.1 CHIEF INFORMATION SECURITY OFFICER (CISO) 7
3.2 CHFS OATS INFORMATION SECURITY (IS) TEAM 7
3.3 CHIEF PRIVACY OFFICER (CPO) 7
3.4 SECURITY/PRIVACY LEAD 7
3.5 CHFS STAFF AND CONTRACTOR EMPLOYEES 7
3.6 INFORMATION SYSTEM PERSONNEL 7

4 POLICY REQUIREMENTS 8

4.1 GENERAL INFORMATION 8
4.2 AUDITING NON-LOCAL MAINTENANCE AND DIAGNOSTIC SESSIONS 8
4.3 MAINTENANCE AND RECORD KEEPING 9
4.4 SESSIONS TERMINATION UPON COMPLETION OF NON-LOCAL MAINTENANCE 10

5 POLICY MAINTENANCE RESPONSIBILITY 10

6 POLICY EXCEPTIONS 10

7 POLICY REVIEW CYCLE 10

8 POLICY REFERENCES 10

1 Policy Definitions

- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation not to 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; 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.
- **Controlled Maintenance**: Tasks performed on an information system or components (software or hardware) which are scheduled and performed in accordance with manufacturer, vendor or agency specifications.
- **Corrective Maintenance**: When a system abruptly fails or generates an error condition, a corrective maintenance task is performed to repair or replace failed components (software or hardware), so the system can be restored to an operational condition as soon as possible. Corrective maintenance may be performed by in-house personnel or outside vendors under a service agreement.
- **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.

- **Non-Local System Maintenance**: Non-Local System Maintenance is interpreted to mean performing remote support via an authenticated network connection. Operators have the option to enable SSH login to PAS VMs using either the BOSH CLI, and/or via any standard SSH client.
- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61.931-934 and in accordance with National Institute of Standards and Technology (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.
- **Preventive Maintenance:** Controlled tasks performed on an information system or components (software or hardware) that are designed to prevent failure are preventive maintenance. Upgrades, patches, or cleaning of parts, components, or materials during off-peak hours are examples of preventive maintenance that minimize information system and component failures.
- **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 : 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) Office of Application Technology Services (OATS) must establish an acceptable level of security controls to implement through a Non-Local maintenance policy. This document establishes the agency's implementation policy related to Non-Local maintenance to manage risks and provide guidelines for security best practices regarding remote maintenance on CHFS information systems.

2.2 Scope

The scope of this policy applies to all internal CHFS state and contract personnel/employees, 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. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

Note: The ownership and maintenance of CHFS IT assets are COT's responsibility. Hence, any policy maintained at the enterprise level or a document developed by COT pertaining to Non-Local maintenance will supersede this policy.

2.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officer, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with other CHFS organizations or agencies with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in 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, IRS, and SSA.

3 CHFS 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 CHFS OATS Information Security (IS) Team

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

3.3 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 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.

3.4 Security/Privacy Lead

Individual(s) is 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 protection of Payment Card Industry (PCI), PII, ePHI, FTI and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

3.5 CHFS Staff and Contractor Employees

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).

3.6 Information System Personnel

Organizational personnel with required access authorizations and technical competence that supervises the maintenance activities and reviews the records of maintenance and diagnostic sessions.

4 Policy Requirements

Individual(s) must adhere to the Non-Local maintenance policy as well as referenced documents 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.

4.1 General Information

This policy describes the requirements to be followed in instances when a Non-Local maintenance activity is being performed on CHFS-designated IT infrastructure.

1. Non-Local maintenance and diagnostic activities shall be performed by COT on the information system and those activities must be authorized, logged, monitored, and controlled.
2. The use of Non-Local maintenance and diagnostic tools must be consistent with the requirement documented within the following policies:
   - CIO-058 - IT Equipment Room Access at the Commonwealth Data Center Policy (This is a COT document. Please reach out to COT to obtain this document.)
   - CIO-059 - Equipment Installation and Removal at the Commonwealth Data Centers Policy (This is a COT document. Please reach out to COT to obtain this document.)
3. CHFS shall allow the use of Non-Local maintenance and diagnostic tools only as consistent with enterprise policy or any other policies developed by COT related to Non-Local maintenance.

4.2 Auditing Non-Local Maintenance and Diagnostic Sessions

1. Non-Local maintenance and diagnostic sessions must be audited, and the designated information system personnel from COT shall review and audit the maintenance records of the sessions. COT is the responsible agency to authorize, log, monitor, control Non-Local maintenance and perform, audit and diagnostic sessions.
2. Identification and authentication techniques must be consistent with the network access requirements found in
   - CIO-074 Enterprise Network Security Architecture Policy
   - 020.301- CHFS Network User Accounts Policy.
3. Access information such as passwords or port information must be communicated by secure means (e.g., encrypted communications, phone).
4. Non-Local executed maintenance and diagnostic activities must not bypass information technology security controls or violate any CHFS or COT policy or standard set forth.
5. Strong identification and authentication techniques in the establishment of Non-

Local maintenance and diagnostic sessions must be employed as prescribed by COT policy or requirements.

6. Any exception should follow CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy. Additionally, the Security Exemption form COT-F085 must be used to request an exemption and submitted to COT via ServiceNow.
7. Staff Service Request Form (and COT Entrance/Exit Form) COT-F181 should be used to request access to various COT administered resources (Mainframe, Home Folder/Shared Folder Permissions, Windows Server Support, Enterprise UNIX Servers, VPN, Database Access, etc.) and submitted to COT via ServiceNow.

4.3 Maintenance and Record Keeping

1. Maintenance records must be maintained by COT for all Non-Local maintenance, diagnostic and service activities. The records shall be retained as per the enterprise retention policy or per the Kentucky Department for Library and Archive (KDLA) retention requirement if a longer retention period is required.
2. When maintenance is to be conducted externally by a third party, the information system personnel shall accomplish the following:
    I. Ensure the required connection features are set by COT
    II. Provide assistance to the third-party individual during the Non-Local connection session and also monitor the process in real time (i.e., as it is happening).
    III. Maintain control of the session at all times. Verify the completion of the Non-Local maintenance and terminate the session.
3. Any maintenance ports, services, and protocols that must be used during Non-Local maintenance, are only permitted to be enabled during maintenance and must be disabled subsequently.
4. The policies and procedures for the establishment and use of Non-Local maintenance and diagnostic connections must be documented in the information system's System Security Plan (SSP).
5. Non-Local maintenance or diagnostic services must be performed from an information system that implements the same level of security (or higher) as that implemented on the information system being serviced.
6. If the above condition cannot be met, then the component to be serviced must be removed from the information system and prior to Non-Local maintenance and diagnostic services, sanitized (with regard to organizational information) before removal from organizational facilities, and it must also be inspected and sanitized (with regard to potentially malicious software and or any other viruses) after the service is performed and before reconnecting the component to any of CHFS's information systems.

4.4 Sessions Termination Upon Completion of Non-Local Maintenance

1. When Non-Local maintenance and diagnostic activities are completed, the following must be adhered to and verified:
    1) All sessions and network connections invoked in the performance of the activity must be terminated upon completion of activities.
    2) All temporarily enabled or opened maintenance ports, services, or protocols must be disabled or closed again upon completion of activities.
    3) Access granted to specifically perform the maintenance activity shall be documented then revoked by COT personnel after the request has been completed.

5 Policy Maintenance Responsibility

The CHFS 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

- 020.301- CHFS Network User Accounts Policy
- 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
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Department for Library and Archive (KDLA)
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Security Exemption Request, COT-F085
- Staff Service Request Form, COT-F181