Commonwealth of Kentucky
Cabinet for Health and Family Services

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

050.102 Information Systems Security Incident Response and Reporting Policy

Version 2.9
July 1, 2024

Revision History

Date	Version	Description	Author
10/1/2006	1.0	Effective Date	CHFS IT Policies Team Charter
07/01/2024	2.9	Review Date	CHFS Policy Charter Team
07/01/2024	2.9	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	7/1/2024	Jeremy Rogers	DocuSigned by: Jeremy Rogers FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or delegate)	7/1/2024	Kelvin Brooks	DocuSigned by: Kelvin Brooks A0F3F24DC182406...

Table of Content

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: 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.
- **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.
- **Personally Identifiable Information (PII):** Defined by 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.

- **Security Breach:** Defined by KRS Chapter 61.931-61.934 as the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted or unencrypted records or data that compromises the security, confidentiality, or integrity of another's personal information or confidential information that result in the likelihood of harm to one (1) or more individuals.
- **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's proprietary information including but not limited to intellectual property, financial data and more.
- **Sensitive Financial Data (including PCI):** Defined by Payment Card Industry (PCI) Data Security Standards (DSS) Security Standards as cardholder and sensitive authentication data including Primary Account Number (PAN), cardholder name, expiration date, service code, full track data (magnetic stripe data or equivalent on a chip0, Card Security Codes such as CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data as anything that is inclusive of bank identification/information (i.e., bank routing number, account number, etc.).
- **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.
- **Third Party**: 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 organization whose capabilities can be determined sufficient to conduct assessment needs.
- **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 level of security controls through an incident response and reporting policy. This document establishes the agency's Information Systems Incident Response and Reporting Policy, which helps manage risks and provide guidelines for security best practices regarding responding to and reporting security incidents.

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. 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.

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

Coordination within CHFS organizations and/or agencies that 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. Additionally, applicable agencies 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 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.

3.3 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 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 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 vendors 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 the adherence of this policy.

3.6 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this procedure. 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 System Data Owner and System Data Administrators

Management/lead, or appointed delegate, who works with the application’s development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas for providing full recovery of all application functionality as well as meeting federal and state regulations for disaster recovery situations.

3.8 Incident Response Coordinator (INCIDENT RC)

The Incident Response Coordinator (INCIDENT RC) receives notifications and news from the CISO and security groups to remain current with the information within security landscape. The INCIDENT RC is responsible for composing and distributing a notification of Cybersecurity related news and events to key CHFS stakeholders. This information is gathered and disseminated to further ensure the identification and handling of potential threats and incidents.

3.9 Office of Attorney General Staff Attorney

The Staff Attorney for the Office of Attorney General oversee all applicable state laws are followed in reference to reportable breaches.

3.10 Finance and Administration Cabinet Secretary

The Finance and Administration Cabinet Secretary tracks all determined breaches to analyze if there is a possible financial impact.

3.11 Kentucky State Police (KSP) Commissioner

The Kentucky State Police Commissioner shall be informed if a breach has been determined, and law enforcement is deemed necessary.

3.12 Auditor of Public Accounts

The Auditor of Public Accounts (APA) job function is to audit the entire state government. They shall be notified of any security breach to correlate and determine if the appropriate response or action has been taken.

3.13 CHFS Office of Communications

The CHFS Office of Communications shall be updated on all confirmed/determined breaches that results in any media coverage regarding the incident/breach.

3.14 CHFS General Counsel

The CHFS General Counsel shall be notified of any determined breaches to ensure governmental agency reporting processes are followed.

4 Policy Requirements

4.1 General Security Incident Response

Any CHFS contractor, state, or vendor staff/personnel who suspects an information security incident must report that incident as soon as possible to their supervisor. The employee or supervisor must contact their designated CHFS agency privacy and/or security liaison/lead, CPO, or the INCIDENT RC from the Security IRP Contacts List as well as the CHFS IS Team at CHFSOATSSecurity@ky.gov to provide information for investigation into the event or incident.

If any employee has questions or concerns regarding information security incidents

within CHFS, they may contact the IS Team as stated above. After the conclusion of each major incident, an After Action Report shall be completed and made available for management review and action.

4.2 Security Incident Reporting

IS Team uses the Security Incident Management module in Archer to log, investigate, and report all security incidents. CHFS adheres to all federal and state requirements regarding the investigation, management and reporting of information security incidents and/or security breaches.

4.3 Health Insurance Portability and Accountability Act (HIPAA)

The Cabinet follows the HIPAA requirements for logging security incidents. Additionally, CHFS investigates potential security breaches as defined under The Health Information Technology for Economic and Clinical Health (HITECH) Act and complies with all reporting requirements as outlined under the HITECH Act. Per the CHFS Business Associate Agreement, the agency must notify the covered entity **within five (5) calendar days** of the discovery of a breach.

When a breach of PHI affects four hundred ninety-nine (499) or fewer individuals, the Privacy Officer, or designee, must log the incident and report to the HHS website within 60 calendar days of the end of the calendar year in which the breach was discovered. For data breaches that affect five hundred (500) or more individuals, the Privacy Officer, or designee, must log the incident and report to the HHS website without unreasonable delay and **in no case no later than sixty (60) calendar days** from the date of the discovery of the breach.

Within the Public Health domain and all areas encompassed, such as laboratories, there are specific exceptions where PHI can be released without consent from a citizen. These exceptions are detailed in the HIPAA Privacy Rule. Refer to the section titled "Permitted PHI Disclosures without Authorization" for details that outline what the precise conditions allow for the release of the PHI.

4.4 Internal Revenue Service (IRS)

The Cabinet follows all security incident requirements for Federal Tax Information (FTI) as outlined in IRS Publication 1075. Upon discovery of a possible improper or suspected inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information must contact the office of the appropriate special agent-in-charge, IRS Office of Safeguards, immediately, but no later than twenty-four (24) hours after identification of a possible issue involving FTI.

The agency must notify the Office of Safeguards by email to the Safeguard mailbox, SafeguardReports@irs.gov within **twenty-four (24) hours.** The Office of Safeguards

will report the incident to the Treasury Inspector General for Tax Administration and concurrent reporting is not required. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to the following:

- Name of agency and agency point of contact for resolving data incident with contact information.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- How the incident was discovered.
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred.
- IT assets involved (e.g., laptop, server, mainframe)

Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term “Data Incident Report” in the subject line of the e-mail. Do not include any FTI in the data incident report.

4.5 Social Security Administration (SSA)

The SSA requires the agency entrusted with SSA supplied PHI and/or PII data to report any suspected or confirmed breach of personal data be reported to their SSA Regional Office Contact and SSA Systems Security Contact **within one (1) hour** of discovery of the incident. If the responsible state official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one (1) hour, the responsible state agency official or delegate must report the incident by contacting SSA’s National Network Service Center (NNSC) toll free at 877-697-4889 (select “Security and PII Reporting” from the options list).
The CHFS agency will provide updates to the SSA contacts as they become available.

4.6 Kentucky Revised Statues (KRS) 61.931 to 61.933

Kentucky Revised Statues (KRS) Chapter 61 §931 to 933 requires that a state agency, or a nonaffiliated third party the agency contracts with, must report a personal information security breach to the officials listed in KRS 61.933(1)(a). The notice of the security breach of personal information shall be in the most expedient time possible and without unreasonable delay but **within seventy-two (72) hours** of determination or notification of the security breach. The length of time is not determined by business days or business hours. The **seventy-two (72) hour** period begins once the Security IRP Contact becomes aware of the notification from the INCIDENT RC. If the notification is sent to the Security IRP Contact on a date when the Security IRP Contact is out of the office, whether due to a weekend, holiday or any other reason, the Security

IRP Contact has 72 hours from the time they become aware of the incident after returning to work to send the initial notification to appropriate contacts.

The notification required by KRS 61.933(1)(a) shall include all information the agency (or nonaffiliated third party) has with regard to the security breach at the time of notification.

The officials within the Security IRP Contacts List that must be notified by e-mail of a security breach, according to KRS 61.933(1) (a) include, but are not limited to the following:

- Office of Attorney General, Staff Attorney
- Finance and Administration Cabinet Secretary
- Kentucky State Police, Commissioner
- Auditor of Public Accounts
- In addition, for CHFS add or forward to:
    - Privacy officer
    - Security Officer
    - Incident Coordinator- INCIDENT RC
    - CHFS Office of Communications
    - CHFS General Counsel

4.7 Other Reporting

More examples of the types of incidents and breaches that could be encountered are covered in the COT CIO-090 Information Security Incident Response Policy.

CHFS is committed to ensuring that the employees tasked with handling security incidents are adequately trained and prepared to handle their incident response duties, please refer to the CHFS Incident Response Plan for more information regarding appropriate processes and steps when dealing with potential incidents. CHFS will periodically perform incident response exercises, but at least once annually. The exercises are conducted in part as training exercises as well as to test the incident response process.

4.8 Employee Responsibility

CHFS employees are responsible for reporting security incidents. The following security incidents must be reported:

- Possible or actual exposure release, alteration, or loss of confidential information
- Giving or telling another person your password.
- Loss or theft of a laptop, desktop computer or handheld data device.
- Loss or theft of external storage devices, like external hard drives, ZIP and flash drives, CDs and DVDs, used for Cabinet business.

- Loss of employee badge or keys.
- Unauthorized use of CDs, DVDs or other removable media to copy confidential information.
- Attempts to obtain confidential information by e-mail or other electronic communication.
- Attempts by unknown sources to persuade users to download infected e-mail or attachments as well as possible phishing e-mails.
- Receipt of unsolicited, unusual or suspicious e-mail or phone calls.
- Unauthorized physical entry into a controlled area that contains confidential information.
- Electronic monitoring of another employee's workstation.

5 Policy Maintenance Responsibility

The 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

Within the Public Health domain and all areas encompassed, such as laboratories, there are specific exceptions when PHI can be released without consent from a citizen.

These exceptions are detailed in the HIPAA Privacy Rule. The section titled Permitted PHI Disclosures without Authorization outlines the precise conditions to allow for the release of the PHI.

7 Policy Review Cycle

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

8 Policy References

- After Action Report
- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.2
- CHFS Plan: CHFS Incident Response Plan (IRP)
- CHFS Policy: 010.102- Data/Media Security Policy
- CHFS Policy: 070.203 Security Exceptions and Exemptions to CHFS Policies and Security Control Policy
- Employee Privacy and Security of Protected Health, Confidential, and Sensitive Information Agreement- CHFS 219 Form

- Enterprise IT Policy: CIO-085- Authorized Agency Contacts Policy
- Enterprise IT Policy: CIO-090- Information Security incident Response Policy
- Enterprise IT Policy: CIO-091- Enterprise Information Security Program Policy
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Internal Revenue Services (IRS) Publication 1075
- Information Technology Management Portal (ITMP)
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statue (KRS) Chapter 61.931-934
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- OHRM Personnel Handbook
- Payment Card industry (PCI) data Security Standard (DSS) Requirements and Security Assessment Procedures Version 3.2.1
- Procurement, Payables, and Asset Tracking System (PPATS)
- Security IRP List
- Social Security Administration (SSA) Security Information
- U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)