



Information Technology (IT) Policy



***050.102 Information Systems Security Incident
Response and Reporting***

**Version 2.1
February 29, 2016**

050.102 Information Systems Incident Response and Reporting	Current Version: 2.1
050.000 Security Awareness	Effective Date: 10/01/2006

Revision History

Date	Version	Description	Author
10/1/2006	1.0	Effective Date	CHFS IT Policies Team Charter
2/29/2016	2.1	Revision Date	CHFS IT Policies Team Charter
2/29/2016	2.1	Review Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Executive Director (or designee)	2/29/2016	Bernard Decker	

Table of Contents

1	050.102 INFORMATION SYSTEMS INCIDENT RESPONSE AND REPORTING.....	4
1.1	PURPOSE.....	4
1.2	SCOPE.....	4
1.3	ROLES AND RESPONSIBILITIES.....	4
1.3.1	<i>Security Lead</i>	4
1.3.2	<i>Privacy Lead</i>	4
1.3.3	<i>CHFS Staff</i>	4
1.4	MANAGEMENT COMMITMENT.....	4
1.5	COORDINATION AMONG ORGANIZATIONAL ENTITIES.....	5
1.6	COMPLIANCE.....	5
2	POLICY REQUIREMENTS.....	5
2.1	GENERAL SECURITY INCIDENT RESPONSE.....	5
2.2	SECURITY INCIDENT REPORTING.....	5
2.2.1	<i>HIPAA</i>	5
2.2.2	<i>IRS</i>	6
2.2.3	<i>SSA</i>	6
2.2.4	<i>Other</i>	6
2.3	EMPLOYEE RESPONSIBILITIES.....	6
2.4	DEFINITIONS.....	7
2.4.1	<i>Confidential Information</i>	7
2.4.2	<i>Security Breach</i>	7
3	POLICY MAINTENANCE RESPONSIBILITY.....	7
4	EXCEPTIONS.....	7
5	POLICY REVIEW CYCLE.....	8
6	REFERENCES.....	8

050.102 Information Systems Incident Response and Reporting	Current Version: 2.1
050.000 Security Awareness	Effective Date: 10/01/2006

1 050.102 Information Systems Incident Responses and Reporting

Category: 050.000 Security Awareness

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Service (OATS) must establish an acceptable level of security controls to be implemented through an incident response and reporting policy. This document establishes the agency's Information Systems Incident Response and Reporting Policy which help manage risks and lays out guidelines for implementing security best practices in regards to responding and reporting security incidents.

1.2 Scope

The scope of this policy applies to all CHFS OATS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. This policy covers the applicable computer and data communication systems owned and administered by CHFS OATS or third party providers under contract with a CHFS agency.

1.3 Roles and Responsibilities

1.3.1 Security Lead

Responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This role is responsible for the adherence of the Information Systems Incident Responses and Reporting Policy.

1.3.2 Privacy Lead

Responsible to provide the security and privacy guidance of sensitive information to all CHFS information technology (IT) staff. This role is responsible for the adherence of the Information Systems Incident Responses and Reporting Policy alongside the Security Lead.

1.3.3 CHFS Staff

Must adhere to the Information Systems Incident Responses and Reporting Policy as well as referenced documents that pertain to reporting, researching, responding, etc. to a security incident.

1.4 Management Commitment

This policy has been approved by OATS Division Directors and the OATS Executive Director. Senior Management supports the objective put into place by this policy.

050.102 Information Systems Incident Response and Reporting	Current Version: 2.1
050.000 Security Awareness	Effective Date: 10/01/2006

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet who access their applications or systems. All organizational entities that interact with OATS are subject to follow guidelines outlined within this policy.

1.6 Compliance

CHFS has chosen to adopt the security awareness and principles established in the National Institute of Standards and Technology (NIST), the Internal Revenue Services (IRS), the Social Security Administration (SSA), the Centers for Medicare and Medicaid Services (CMS), as well as other federal and state organizations as the official guidance domain for this policy.

2 Policy Requirements

2.1 General Security Incident Response

Any CHFS employee who suspects an information security incident (under Employee Responsibilities) must report that incident as soon as possible to their supervisor and to the Office of Administrative and Technology Services (OATS) Office of the Executive Director. They may contact the OATS Office of the Executive Director or the CHFS IT Security and Audit Team at CHFSSecurityTeam@ky.gov.

If any employee has questions or concerns regarding information security incidents within the Cabinet, they may contact the CHFS IT Security and Audit Team as listed above. After the conclusion of each incident, a post incident analysis report will be completed and made available for management review and action.

2.2 Security Incident Reporting

OATS uses the Security Report Tracking Log data base 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.

2.2.1 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 5 calendar days** of the discovery of a breach.

When Protected Health Information (PHI) and 499 or fewer records are involved, the

050.102 Information Systems Incident Response and Reporting	Current Version: 2.1
050.000 Security Awareness	Effective Date: 10/01/2006

Privacy Officer, or designee, must log the incident and report to The US Department of Health and Human Services (HHS) website, at least annually. For data breaches of 500 or more records, the Privacy Officer, or designee, must report to the HHS website once the breach and number of records are confirmed.

2.2.2 Internal Revenue Service (IRS)

The Cabinet follows all security incident requirements for Federal Tax Information (FTI) as outlined in IRS Publication 1075. The Treasury Inspector General for Tax Administration (TIGTA) must be notified immediately, **but no later than 24 hours after** the identification of a possible issue involving FTI is discovered. CHFS will contact Kentucky's TIGTA Field Division in Chicago at 312-554-8751.

2.2.3 Social Security Administration (SSA)

The SSA requires the agency entrusted with SSA supplied with Protected Health Information (PHI) and/or Personally Identifiable Information (PII) data report any suspected or confirmed breach of personal data be reported to their SSA Regional Office Contact and SSA Systems Security Contact **within one hour** of discovery of the incident.

If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one 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 as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

2.2.4 Other

More examples of the types of incidents and breaches which 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.

CHFS will periodically perform incident response exercises. The exercises are conducted in part as training exercises and to test the incident response process.

2.3 Employee Responsibility

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

050.102 Information Systems Incident Response and Reporting	Current Version: 2.1
050.000 Security Awareness	Effective Date: 10/01/2006

- Possible or actual exposure release, alteration or loss of confidential information
- Giving or telling another person your password.
- Loss or theft of a laptop or 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.
- 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.
- 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.

2.4 Definitions

2.4.1 Confidential Information

Any information that pertains to identifying a person by name, address, social security number, or other forms of personal identification; including Protected Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information (FTI) or Internal Revenue Services (IRS) provided Data, Social Security Administration (SSA) provided Data, Centers for Medicare and Medicaid Services (CMS) provided data, Health Insurance Portability and Accountability Act (HIPAA) provided data, and other federally provided personal data.

2.4.2 Security Breach

The unauthorized acquisition, distribution, disclosure, or release of encrypted or unencrypted records or data that compromises the security, confidentiality, or integrity of another's personal information or confidential information.

3 Policy Maintenance Responsibility

The Office of Administrative and Technology Services (OATS) IT Security & Audit Section is responsible for the maintenance of this policy.

4 Exceptions

There are no exceptions to this policy.

050.102 Information Systems Incident Response and Reporting	Current Version: 2.1
050.000 Security Awareness	Effective Date: 10/01/2006

5 Policy Review Cycle

Annual

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS IT Policy: 010.102- Data Media Security Policy
- CHFS OHRM Personnel Handbook
- CHFS 219 Confidentiality Agreement
- Enterprise IT Policy: CIO-085- Agency Security Contact
- 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 (HIPAA) of 1996
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Health Benefit and Information Exchange (KHBE) Incident Response Plan
- National Institute of Standards and Technology (NIST) Special Publications (SP) document 800-30- Risk Management Guide for Information Technology 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) Framework