



***Information Technology (IT) Policy***



***050.103 System's Security Plan***

**Version 1.1**  
**April 29, 2016**

050.103 System's Security Plan	Current Version: 1.1
050.000 Security Awareness	Effective Date: 4/29/2016

## Revision History

Date	Version	Description	Author
4/29/2016	1.1	Effective Date	CHFS IT Policies Team Charter
4/29/2016	1.1	Revision Date	CHFS IT Policies Team Charter
4/29/2016	1.1	Review Date	CHFS IT Policies Team Charter

## Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	4/29/2016	Robert Purr CIO	

050.103 System's Security Plan	Current Version: 1.1
050.000 Security Awareness	Effective Date: 4/29/2016

## Table of Contents

- 1 050.103 SYSTEM'S SECURITY PLAN..... 4**
- 1.1 PURPOSE..... 4
- 1.2 SCOPE..... 4
- 1.3 ROLES AND RESPONSIBILITIES..... 4
  - 1.3.1 Security Lead..... 4
  - 1.3.2 Privacy Lead..... 4
  - 1.3.3 CHFS Staff..... 4
- 1.4 MANAGEMENT COMMITMENT..... 4
- 1.5 COORDINATION AMONG ORGANIZATIONAL ENTITIES..... 4
- 1.6 COMPLIANCE..... 5
- 2 POLICY REQUIREMENTS..... 5**
- 2.1 SYSTEM SECURITY PLAN..... 5
- 2.2 RULES OF BEHAVIOR..... 6
- 2.3 INFORMATION SECURITY ARCHITECTURE..... 6
- 3 POLICY MAINTENANCE RESPONSIBILITY..... 6**
- 4 EXCEPTIONS..... 6**
- 5 POLICY REVIEW CYCLE..... 6**
- 6 REFERENCES..... 7**



050.103 System's Security Plan	Current Version: 1.1
050.000 Security Awareness	Effective Date: 4/29/2016

# 1 050.103 System's Security Plan

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 a security planning policy. This document establishes the System's Security Planning Policy, for managing risks and guidelines for implementing security best practices with regards to security planning, preparation, and strategy.

## 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

The security lead is responsible for assessing, planning and implementing all required security standards. This role is responsible for adhering to the System's Security Planning Policy.

### 1.3.2 Privacy Lead

The privacy lead is responsible for providing the security and privacy guidance of sensitive information to all CHFS information technology (IT) staff. This role is responsible for adhering to the System's Security Planning Policy together with the Security Lead.

### 1.3.3 CHFS Staff

CHFS Staff must adhere to the System's Security Planning Policy as well as referenced documents that pertain to security planning.

## 1.4 Management Commitment

This policy has been approved by OATS Division Directors and the OATS Chief Information Officer (CIO). Senior Management supports the objective put into place by this policy.

## 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 planning 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 System Security Plan

CHFS OATS must develop and maintain a System Security Plan (SSP) for the agency's information system. An approved and accurate System Security Report (SSR), from the IRS satisfies the requirement for a SSP, for those applications that use Federal Tax Information (FTI).

This plan will delineate responsibilities and expected behavior of all individuals who access the applications. The SSP/SSR should be viewed as documentation and processes for the security protections of information systems, including those that contact FTI.

The agency will develop a system security plan that includes the following guidelines:

1. A plan that is consistent with the organization's enterprise architecture
2. A plan that explicitly defines the authorization boundary for the system
3. A plan that describes the operational context of the information system in terms of missions and business processes
4. A plan that provides the security categorization of the information system including supporting rationale
5. A plan that describes the operational environment for the information system and relationships with or connections to other information systems
6. A plan that provides an overview of the security requirements for the system
7. A plan that identifies any relevant overlays, if applicable
8. A plan that describes the security controls in place or planned for meeting those requirements including a rationale for tailoring decisions
9. A plan that is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

The SSP/SSR will be reviewed at least annually or more often if there are major changes in the system. The agency will share the plan updates and changes with all necessary agency management staff as needed or upon request.

Reasons for changes or updates to the plan may include:

1. Changes to the information systems

050.103 System's Security Plan	Current Version: 1.1
050.000 Security Awareness	Effective Date: 4/29/2016

2. Change to the environment of operations
3. Change or updates to security controls in place
4. Problems identified during plan implementations or security control assessments
5. Other major releases or changes to the system or application

Agencies may develop procedures to plan and coordinate security related activities regarding the information system with affected stakeholders before conducting such activities to reduce the impact on other organizational entities.

## **2.2 Rules of Behavior**

CHFS OATS will establish, provide, describe, and make readily available the responsibilities and expected behavior to individuals who require access to the information system.

An appointed OATS staff member, or appointed group, will be responsible for updating the rules of behavior at least annually. Initially and annually thereafter individuals will also be required to sign an acknowledgement form- such as the CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS 219)- agreeing that they have read, understood, and agree to abide by the rules of behavior before accessing the system or application.

## **2.3 Information Security Architecture**

The agency will develop the information security architecture for the information system. This architecture will describe the overall requirements of how the agency plans to protect the confidentiality, integrity, and availability of the information. This security architecture will be updated to reflect updates in the enterprise architecture. All changes and updates will be documented in the SSP/SSR, when applicable.

## **3 Policy Maintenance Responsibility**

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

## **4 Exceptions**

Any exceptions to this policy must follow the procedures established in CHFS IT Policy: 070.203.

## **5 Policy Review Cycle**

Annual

050.103 System's Security Plan	Current Version: 1.1
050.000 Security Awareness	Effective Date: 4/29/2016

## 6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS 219)
- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- CHFS IT Security Planning Procedure
- Internal Revenue Services (IRS) Publications 1075
- National institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National institute of Standards and Technology (NIST) Special Publication 800-12 An Introduction to Computer Security
- 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