



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



**040.201 Internal Risk Assessment**

**Version 1.0**  
**April 29, 2016**

040.201 Internal Risk Assessment	Current Version: 1.0
040.000 Contingency Planning/Operations	Effective Date: 4/29/2016

## Revision History

Date	Version	Description	Author
4/26/2016	1.0	Effective Date	CHFS IT Policies Team Charter
4/29/2016	1.0	Revision Date	CHFS IT Policies Team Charter
4/29/2016	1.0	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 E PUTT CIO	

040.201 Internal Risk Assessment	Current Version: 1.0
040.000 Contingency Planning/Operations	Effective Date: 4/29/2016

## Table of Contents

<b>1</b>	<b>040.201 INTERNAL RISK ASSESSMENT .....</b>	<b>4</b>
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 .....	5
1.5	COORDINATION AMONG ORGANIZATIONAL ENTITIES .....	5
1.6	COMPLIANCE .....	5
<b>2</b>	<b>POLICY REQUIREMENTS.....</b>	<b>5</b>
2.1	RISK ASSESSMENT CONTROLS VERIFICATION AND ASSESSMENT .....	5
2.2	BUSINESS PARTNER ASSESSMENT.....	6
2.3	TECHNICAL VULNERABILITY SCANNING AND PENETRATION TESTING .....	6
2.4	APPLICATION SECURITY ASSESSMENT.....	6
2.5	THREAT MONITORING .....	6
2.6	SECURITY CATEGORIZATION .....	7
<b>3</b>	<b>POLICY MAINTENANCE RESPONSIBILITY .....</b>	<b>7</b>
<b>4</b>	<b>EXCEPTIONS .....</b>	<b>7</b>
<b>5</b>	<b>POLICY REVIEW CYCLE .....</b>	<b>7</b>
<b>6</b>	<b>REFERENCES .....</b>	<b>7</b>

040.201 Internal Risk Assessment	Current Version: 1.0
040.000 Contingency Planning/Operations	Effective Date: 4/29/2016

# 1 040.201 Internal Risk Assessment

Category: 040.000 Contingency Planning/Operations

## 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 risk assessment policy. This document establishes the Internal Risk Assessment Policy, for managing risks and guidelines for implementing security best practices with regards to risk assessments, 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

### 1.1.1 Security Lead

The security lead is responsible for assessing, planning and implementation all required security standards. This role is responsible for adhering to the Internal Risk Assessment Policy through:

- Providing consultation, coordination, and approval activities for risk assessment standards, related procedures and remediation activities.
- Defining and maintaining the final risk assessment report(s) and related documents in which risk assessment results are recorded and published.
- Developing and maintaining procedures for conducting information system risk assessments.
- Conducting a formal risk assessment annually to evaluate potential risks applicable for each in-scope system(s).

### 1.1.2 Privacy Lead

The privacy lead provides security and privacy guidance of sensitive information to all CHFS information technology (IT) staff. This role is responsible for adhering to the Internal Risk Assessment Policy together with the Security Lead.

### 1.1.3 CHFS Staff

CHFS staff must adhere to the Internal Risk Assessment Policy as well as any referenced documents pertaining to all aspects of a risk assessment.

040.201 Internal Risk Assessment	Current Version: 1.0
040.000 Contingency Planning/Operations	Effective Date: 4/29/2016

## **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 mandated 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**

The CHFS agency must assess the risk to information systems confidentiality, integrity, and availability through execution of the following:

- Risk Assessment
- Business Partner Assessments
- Technical Vulnerability Scanning and Penetration Testing
- Application Security Assessment
- Threat Monitoring

The CHFS executive leadership along with business partners and other stakeholders shall define the agency's critical systems that are subject to meet the assessments listed and defined within this policy.

## **2.1 Risk Assessment Controls Verification and Assessment**

The CHFS agency will complete an annual verification and risk assessment which includes the following:

- Identifies gaps in compliance for areas of risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits
- Identifies the need for enhanced and/or additional controls

The CHFS agency will also assess defined controls if there is an increase or major

040.201 Internal Risk Assessment	Current Version: 1.0
040.000 Contingency Planning/Operations	Effective Date: 4/29/2016

changes to the agency's information system. The Cabinet's Chief Information Officer (CIO), or designee, will define and maintain test requirements within the Risk Assessment IET Framework for reach control.

All Risk assessment results will be reviewed, documented, reported, labeled, handled, and retained as classified. Risk assessments will be shared with appropriate parties within the agency. Reports and findings shall be subject to reporting requirements as established by applicable laws, executive orders, directives, policies, regulations, standards, and/or other state and federal guidelines.

## **2.2 Business Partners Assessment**

A Business Partner risk assessment will be conducted for partners that:

- Have physical custody of the agency's system information components assigned to a Security Impact Category of Moderate or higher.

A Business Partner Risk Assessment will be reviewed for partners at least annually or if the following conditions arise:

- Under consideration for work with the CHFS agency's information systems before connecting to the system or before information is shared with the partner.
- At the discretion of the CIO, or designee, in cases of ad-hoc reviews or as desired.

## **2.3 Technical Vulnerability Scanning and Penetration Testing**

CHFS complies with and adheres to the Commonwealth Office of Technology (COT) Policy CIO-082, Critical Systems Vulnerability Assessments for scanning of the agency's infrastructure.

The CHFS executive leadership along with business partners and other stakeholders shall define the agency's critical systems that are subject to meet the assessments listed and defined within this policy.

## **2.4 Application Security Assessment**

The CHFS Security Architect, an approved third party vendor, or CIO appointed contact is responsible for conducting application security assessment(s). Security assessment(s) must be conducted on each agency's application(s) as defined by federal and state guidelines governing the agency.

## **2.5 Threat Monitoring**

Reference Application Security Assessment (Section 2.4).

040.201 Internal Risk Assessment	Current Version: 1.0
040.000 Contingency Planning/Operations	Effective Date: 4/29/2016

## 2.6 Security Categorization

Risk levels (i.e. Critical, High, Moderate, and Low) put in place by the OATS IT Security and Compliance Team, are defined by federal and state guidelines, Executive Orders, directive, policies, regulations, standards, and guidance governing each agency. Each agency must remediate all vulnerabilities within the federally defined timeline per risk category level. Security categorization results (including supporting rationale) will be documented within the agency's System Security Plan/ System Security Report (SSP/SSR).

## 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

## 6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS IT Policy: 065.004- New Application Development Policy
- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- CHFS Risk Assessment Program Procedure
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments Policy
- Internal Revenue Services (IRS) Publication 1075
- 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