



Information Technology (IT) Policy



020.206 Certification and Accreditation

Version 2.1
September 16, 2016

020.206 Certification and Accreditation	Current Version: 2.1
020.000 Managerial Security	Effective Date: 12/16/2011

Revision History

Date	Version	Description	Author
12/16/2011	1.0	Effective Date	CHFS IT Policies Team Charter
9/16/2016	2.1	Revision Date	CHFS IT Policies Team Charter
9/16/2016	2.1	Review Date	CHFS IT Policies Team Charter

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	9/16/2016	Robert Pitt	

020.206 Certification and Accreditation	Current Version: 2.1
020.000 Managerial Security	Effective Date: 12/16/2011

Table of Contents

1	020.206 CERTIFICATION AND ACCREDITATION	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 INFORMATION.....	5
2.2	SECURITY ASSESSMENTS	5
2.3	PLAN OF ACTION AND MILESTONES (POA&M).....	5
2.4	RESPONSIBILITY	6
2.5	COMPLETION AND APPROVAL PROCESS	6
3	POLICY MAINTENANCE RESPONSIBILITY	6
4	EXCEPTIONS.....	6
5	POLICY REVIEW CYCLE.....	6
6	REFERENCES	6

020.206 Certification and Accreditation	Current Version: 2.1
020.000 Managerial Security	Effective Date: 12/16/2011

1 020.206 Certification and Accreditation

Category: 020.000 Managerial Security

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to implement through a certification and accreditation policy. This document establishes the agency's Certification and Accreditation Policy which helps manage risks and provides guidelines for security best practices regarding the review and appropriate maintenance of the agency's information system.

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. This policy excludes third-party (vendor) managed systems.

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 Certification and Accreditation Policy.

1.3.2 Privacy Lead

Responsible for the provision of security and privacy guidance, of sensitive information, to all CHFS information technology (IT) staff. This role is responsible for the adherence of the Certification and Accreditation Policy alongside the Security Lead.

1.3.3 CHFS Staff

Must adhere to the Certification and Accreditation Policy as well as referenced documents that pertain to the agency's applications.

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.

020.206 Certification and Accreditation	Current Version: 2.1
020.000 Managerial Security	Effective Date: 12/16/2011

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet which access applications or systems. All organizational entities that interact with CHFS systems are subject to follow requirements outlined within this policy.

1.6 Compliance

CHFS abides by the security and privacy requirements 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 Information

CHFS will certify and accredit any information systems, within OATS, that employs sensitive information, annually. Certification, accreditation, and security/risk assessments will be used to ensure appropriate levels of controls exist, they are managed, and are compliant with all federal and state laws and regulations. CHFS will ensure the most current baseline security requirements, as defined by National Institute of Standards and Technology (NIST) 800-53, are met.

2.2 Security Assessments

Per NIST 800-53, all application systems deemed critical by CHFS executive leadership, business partners, and other stakeholders, will at a minimum, annually undergo a partial or full security and privacy assessment. An assessment report will be generated with the results of the assessment. The assessment will be reviewed and approved by the appropriate Agency/Business Owner and results will be shared with parties deemed appropriate.

2.3 Plan of Action and Milestones (POA&M)

Per NIST 800-53, all application systems deemed critical by CHFS executive leadership, business partners, and other stakeholders, will develop a Plan of Action and Milestones (POA&M). Findings and corrections, based on any audits, security impact analyses, monitoring activities or other review types, shall be documented and tracked in the Agency's POA&M. This will reduce or eliminate known vulnerabilities in the system.

020.206 Certification and Accreditation	Current Version: 2.1
020.000 Managerial Security	Effective Date: 12/16/2011

The POA&M must be monitored and kept up to date on a regular basis. Please refer to the internal POA&M Process established for agencies whom report to the Internal Revenue Service (IRS) or Centers for Medicare and Medicaid Services (CMS) for more actions.

2.4 Responsibility

The OATS IT Security and Compliance Team is responsible for oversight of vulnerability assessments of each system covered by this policy. If a third party is used, the OATS IT Security and Compliance Team is responsible to ensure that the vendor is a qualified organization as determined by COT.

2.5 Completion and Approval Process

The certification and accreditation process is performed by the OATS IT Security & Compliance Team. A senior level executive or manager will be appointed to authorize each agency's information system. Annually, the appointed executive or manager will validate the information system is approved before commencing operations.

This policy also aligns with all OATS and COT Enterprise policies pertaining to Data/Media Security.

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

This policy is reviewed and/or revised on an as needed basis, but at least once annually.

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS IT Policy: 040.201- Internal Risk Assessment Policy
- CHFS IT Policy: 065.014- Division of Systems Management System Development Lifecycle Policy

020.206 Certification and Accreditation	Current Version: 2.1
020.000 Managerial Security	Effective Date: 12/16/2011

- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- CHFS IT Process: CHFS POAM Process
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments
- 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