



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



**020.303 Security Banner**

**Version 2.1**  
**September 16, 2016**

020.303 Security Banner	Current Version: 2.1
020.300 Administrative Security	Effective Date: 08/02/2002

## Revision History

Date	Version	Description	Author
8/2/2002	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 Putt	

020.303 Security Banner	Current Version: 2.1
020.300 Administrative Security	Effective Date: 08/02/2002

## Table of Contents

<b>1</b>	<b>020.303 SECURITY BANNER</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	4
1.5	COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.6	COMPLIANCE	5
<b>2</b>	<b>POLICY REQUIREMENTS</b>	<b>5</b>
2.1	GENERAL	5
2.1.1	<i>Warning Banner Criteria</i>	5
2.1.2	<i>IRS Warning Banner Criteria</i>	5
2.2	BANNER MAINTENANCE	6
2.3	WORKSTATION WARNING BANNER SAMPLE	6
<b>3</b>	<b>POLICY MAINTENANCE RESPONSIBILITY</b>	<b>6</b>
<b>4</b>	<b>EXCEPTIONS</b>	<b>6</b>
<b>5</b>	<b>POLICY REVIEW CYCLE</b>	<b>6</b>
<b>6</b>	<b>REFERENCES</b>	<b>7</b>

020.303 Security Banner	Current Version: 2.1
020.300 Administrative Security	Effective Date: 08/02/2002

# 1 020.303 Security Banner

Category: 020.300 Administrative 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 Security Banner Policy. This document establishes the agency's Security Banner which helps manage risks and provides guidelines for security best practices regarding security banner notification content.

## 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 to the Security Banner 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 Security Banner Policy alongside the Security Lead.

### 1.3.3 CHFS Staff

Must adhere to the Security Banner 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.

020.303 Security Banner	Current Version: 2.1
020.300 Administrative Security	Effective Date: 08/02/2002

## **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 Banner Information**

CHFS complies with and adheres to the Commonwealth Office of Technology (COT) Security Standard Processes Manual (SSPM) as well as governing agencies in regards to context in warning banners.

### **2.1.1 Warning Banner Criteria**

Per the SSPM section 8.3, Access Control and Accountability Log-in, screens will include a special security notice. This notice must state: (1) the system may only be accessed by authorized users; (2) users who access the system beyond the warning page represent that they are authorized to do so; (3) unauthorized system usage or abuse is subject to criminal prosecution; and (4) system usage may be monitored and logged. The following subsections detail the access controls and accountability security policies.

### **2.1.2 IRS Warning Banner Criteria**

Access to IRS Federal Tax Information (FTI), enterprise wide, will contain a warning banner with elements regulated within IRS Publication 1075 Exhibit 8. The following elements must be contained with the warning banner: (1) the system contains U.S. Government information, (2) user actions are monitored and audited, (3) unauthorized use of the system is prohibited, and (4) unauthorized use of the system is subject to criminal and civil sanctions.

Users logging onto CHFS workstations through Virtual Private Network (VPN) are subject to accept/agree to the IRS Publication 1075 Exhibit 8 warning banner criteria as stated above, before access is granted.

020.303 Security Banner	Current Version: 2.1
020.300 Administrative Security	Effective Date: 08/02/2002

## **2.2 Banner Maintenance**

It is the responsibility of COT to install and maintain this security banner on all CHFS equipment.

## **2.3 Workstation Warning Banner Sample**

The below text shall be displayed on all CHFS workstations, at logon, to inform staff that such monitoring may occur without warning.

### **WARNING**

**NOTICE:** This is a government computer system and is the property of the Commonwealth of Kentucky. It is for authorized use only regardless of time of day, location or method of access. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on the system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized state government and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such at the discretion of the Commonwealth of Kentucky. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. The unauthorized disclosure of Data containing privacy or health data may result in criminal penalties under Federal authority. By clicking "OK" you acknowledge your awareness of and consent to these terms and conditions of use.

## **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.

020.303 Security Banner	Current Version: 2.1
020.300 Administrative Security	Effective Date: 08/02/2002

## 6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS IT Policy: 070.203- Exceptions to Standards and Policies Policy
- Enterprise IT Security Standards Processes Manual (SSPM)- Section 8.3 Access Control and Accountability Log-in
- Internal Revenue Services (IRS) Publications 1075
- Internal Revenue Services (IRS) Publication 1075 Exhibit 8
- 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