



***Information Technology (IT) Policies***



***070.102 Unauthorized Hardware/Software***

**Version 2.0**  
**October 14, 2015**

070.102 Unauthorized Hardware/Software	Current Version: 2.0
070.000 Administrative	Effective Date: 09/01/2002

## Revision History

<b>Date</b>	<b>Version</b>	<b>Description</b>	<b>Author</b>
9/1/2002	1.0	Effective Date	CHFS IT Policies Team Charter
10/14/2015	2.0	Revision Date	CHFS IT Policies Team Charter
10/14/2015	2.0	Review Date	CHFS IT Policies Team Charter

070.102 Unauthorized Hardware/Software	Current Version: 2.0
070.000 Administrative	Effective Date: 09/01/2002

## Table of Contents

<b>070.102 UNAUTHORIZED HARDWARE/SOFTWARE .....</b>	<b>4</b>
1.1 POLICY .....	4
1.2 SCOPE.....	4
1.3 POLICY/PROCEDURE MAINTENANCE RESPONSIBILITY .....	4
1.4 APPLICABILITY .....	4
1.5 EXCEPTIONS.....	4
1.6 DEFINITIONS .....	5
1.7 REVIEW CYCLE .....	5
1.8 CROSS REFERENCES.....	5



070.102 Unauthorized Hardware/Software	Current Version: 2.0
070.000 Administrative	Effective Date: 09/01/2002

## **070.102 Unauthorized Hardware/Software**

Category: 070.000 Administration

### **1.1 Policy**

Unauthorized hardware and software will not be permitted on the CHFS network for security reasons and to keep standardized hardware and software configuration on the Cabinet IT network. Any violation of this policy may result in disciplinary action, up to and including dismissal.

### **1.2 Scope**

This policy applies to all CHFS employees and contractors, including all persons providing contractor services, who use, process, or store computerized data relevant to agency business on a CHFS maintained server. This user is responsible for any unauthorized hardware or software placed on the CHFS network and may face disciplinary action including and up to dismissal for violating this policy.

### **1.3 Policy/Procedure Maintenance Responsibility**

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

### **1.4 Applicability**

All CHFS employees and contractors shall adhere to the following policies.

### **1.5 Exceptions**

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

### **1.6 Definitions**

For the purpose of this policy the following definitions apply:

070.102 Unauthorized Hardware/Software	Current Version: 2.0
070.000 Administrative	Effective Date: 09/01/2002

**Unauthorized Hardware and Software** shall be defined as any equipment or software not on the CHFS or Enterprise IT standards list or not approved by the CHFS Chief Information Officer (CIO) or designee.

## **1.7 Review Cycle**

Annual

## **1.8 Cross Reference(s)**

- CHFS IT Policy #010.102 – Data/Media Security
- CHFS IT Policy #070.203 – Exceptions to Standards and Policies
- CHFS Standards List