FIRST HERITAGE FINANCIAL, LLC

INFORMATION SERVICES SECURITY TRAINING POLICY

Maintenance and
Update Responsibility: CIO American Heritage FCU

Information Services Security Training Policy

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

Purpose

The purpose of the Security Training Policy is to describe the requirements for ensuring each user of FHF information systems receives adequate training on computer security issues.

Definitions

Information Systems: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Services (IS): The Information Services Group is responsible for computers, networking and data management.

Policy

- All new users must attend an approved Security Awareness training class prior to, or at least within 30 days of, being granted access to any of FHF information systems.
- All users must sign an acknowledgement stating they have read and understand FHF requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect FHF information systems.
- ~~IS must prepare, maintain, and distribute one or more information security manuals that concisely describe FHF information security policies and procedures.~~
- All users (employees) must be provided with sufficient training and supporting reference materials to allow them to properly protect FHF information systems.
- All users must attend an annual computer security compliance seminar and pass the associated examination.

(IS) must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest in a timely manner.