WARNING

This file contains proprietary information which is highly confidential.

Use discretion in distributing copies.
Hard copies must be shredded before discarding.

FIRST HERITAGE FINANCIAL, LLC

INFORMATION SECURITY

I. Password Policy

II. Risk Assessment Policy

III. Third-Party IT Service Organization Policy

I. Password Policy

Issue Date: October 2011
Revision Date:

---

1. Policy Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of FHF's entire corporate network. As such, all FHF employees (including contractors and vendors with access to FHF systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Policy Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Policy Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any FHF facility, has access to the FHF network, or stores any non-public FHF information.

4. Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
- All production system-level passwords must be part of the security administered global password management database.
- All user-level passwords (e.g., e-mail, Web, desktop computer, etc.) must be changed at least quarterly. The recommended change interval is every two months.
- ~~User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.~~
- In accordance with best security practices, all end user accounts that have system level privileges granted through group memberships or programs are strongly encouraged to establish and maintain a unique password from all other accounts held by that user. Since passwords are encrypted and consequently unknown to IS Management, the effective implementation of this best practice is not measurable.
- ~~Passwords must not be inserted into e-mail messages or other forms of electronic communication.~~

- Password Issuance - When the credit union issues a password to an end user or third party, the preferred method is to provide the password verbally over the phone, but that may not always be an optimal method of transfer. Care must be taken to ensure that the person receiving the password is the intended recipient. If verbal method is not feasible, the password may be issued using secure e-mail.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication unless the email itself is properly encrypted per the Credit Union's encryptions policy. Passwords are sometimes required to be sent to different vendors for a variety of uses. There is no current way to monitor password transfer so the next best option is to require sufficient encryption.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system," and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Policy Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at FHF. Some of the more common uses include: user level accounts, web accounts, e-mail accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords that are used only once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:

— Names of family, pets, friends, co-workers, fantasy characters, etc.

— Computer terms and names, commands, sites, companies, hardware, software

— The words "FHF" or any derivation

— Birthdays and other personal information such as addresses and phone numbers

— Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

— Any of the above spelled backwards

— Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Note: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for FHF accounts as for other non-FHF access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various FHF access needs. For example, select one password for the network systems and a separate password for credit union application systems. Also, select a separate password to be used for an NT account and a AS/400 or UNIX account.

Do not share FHF passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential FHF information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an e-mail message.
- Don't reveal a password to the boss.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.

If someone demands a password, refer them to this document or have them call someone in the security department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every three months (except system-level passwords, which must be changed monthly). The recommended change interval is every two months.

If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications should:

- Support authentication of individual users, not groups.
- Not store passwords in clear text or in any easily reversible form.
- Provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Support TACACS+, RADIUS, and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the FHF Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key, which is known by all, and the private key, which is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

II. Risk Assessment Policy

1. Policy Purpose

To empower senior management and/or internal audit to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability and to initiate appropriate remediation.

2. Policy Scope

Risk assessments can be conducted on any entity within FHF or any outside entity that has signed a *Third-Party Agreement* with FHF. RAs can be conducted on any information system, including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3. Policy Description

The execution, development and implementation of remediation programs are the joint responsibility of senior management and/or internal audit and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the senior management and/or internal audit risk assessment team in the development of a remediation plan.

4. Risk Assessment Process

An audit of internal controls of the IS Department may be conducted at least annually as part of the annual CPA audit, if the CPA firm deems it necessary. A 3rd party contractor will also conduct an intrusion test of all networks annually. Senior management and/or internal audit should conduct RA's of individual departments at least every 24 months. The department RA's may be random or by set schedule. All staff will be required to comply with any remedial action or findings.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions

Terms	Definitions
Entity	Any business unit, department, group, or third party, internal or external to FHF, responsible for maintaining FHF assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of FHF's key information assets and systems. Senior management is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

III. Third-Party IT Service Organization Policy

1. Policy Purpose

This document describes information security requirements for third-party IT service organizations that engage with FHF. A third-party IT service organization is defined as a technology that manages and delivers application capabilities to multiple entities from a data center across a wide area network (WAN) or Virtual Private Network (VPN), such as application service providers (ASP) and hosting service organization (HSO).

2. Policy Scope

This policy applies to any use of third-party IT service organizations by FHF, independent of where hosted.

3. Policy Description

3.1 Requirements of Project Sponsoring Department

The project-sponsoring department must first establish that its project is an appropriate one for the ASP model, prior to engaging any additional infrastructure teams within FHF or ASPs external to the financial institution. The person/team wanting to use the ASP service must confirm that the ASP chosen to host the application or project complies with this policy. The business function to be outsourced must consider the following:

- In the event that FHF data or applications are to be manipulated by, or hosted at, an ASP's service, the business function must have written, explicit permission from the financial institution.
- If the ASP provides or receives confidential information to or from FHF, the project-sponsoring department is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application.
- The ASP must be contractually bound to the Security Standards

3.2 Requirements of the Application Service Provider

The ASP must demonstrate compliance with, and be contractually bound by the following standards in order to be considered for use:

- Ensure the confidentiality, integrity, and availability of all electronic protected financial and personal information that FHF creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.

- Ensure compliance with the security standards by its work force.

Management may request that additional security measures are implemented in addition to the measures stated above, depending on the nature of the project. Management may change the requirements over time, and the ASP is expected to comply with these changes.

ASPs that do not meet these requirements may not be used for FHF projects and processing.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Application service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5. Definitions

Terms	Definitions
Application service provider (ASP)	ASPs combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to an FHF-owned and operated application.
Project sponsoring department	The group within FHF that wishes to utilize the services of an ASP.
Business function	The business need that a software application satisfies managed by an ASP that hosts an application on behalf of FHF.