Table of Contents
Aspire to Excellence
Information Technology
Section (1-I)

FOHFS	Fountain of Hope Family Services Inc. Policy Type:- **Aspire to Excellence** Subject:- Information Technology Section:- **(1.I)** Approval By:- **Michael Oladipo**	**Policy and Procedures** Policy# **ATE-146** Adopted:-**05/06/2014** Effective:-**06/11/2015** Revised:-**08/15/2020**

It is my pleasure to present **FOHFS Agency** Information Technology Strategic Plan for **2019-2022**. The Technology Plan provides a **blueprint** for achieving the vision of **leveraging** reliable and emerging technologies and information resources to support the mission of the Agency.

Executive Summary

The purpose of the Information Technology Strategic Plan is to leverage information technology to advance the mission of the **FOHFS Agency**, to help achieve the goals identified in **FOHFS Agency** Strategic Plan, and to shape the future direction for information technology (IT) initiatives to create a competitive advantage for the **FOHFS Agency**. The Technology Plan is the culmination of an in-depth process that involved strategic thinking, and Research. The Plan will provide direction and set IT priorities for the next four years.

▸ Vision

The vision of **FOHFS** Information Technology Strategic Plan is to leverage reliable and emerging technologies and information resources to support innovative and adaptable teaching, learning, and research, and efficient business operations.

▸ Hardware and Software

(FOHFS Agency) uses desktop computers, which are password protected. Basic software such as Microsoft Office products is used on the computers. Staff is not allowed to down load any type of software without the permission of **the Technical/Compliance Officer**. Currently the agency bill directly trough **Millennium Medical System** (**MMS**) a web based behavioral health application software. The software is used to complete **Intake Assessment**, **Treatment Plans**, **Progress Notes**, and **Electronic billing**. This system is maintained by **Millennium Medical System Inc.**

▸ Backup Policies

Purpose and Scope

The purpose of this policy is as follows:

1. To safeguard the information assets of **FOHFS Agency**
2. To prevent the loss of data in the case of an accidental deletion or corruption of data, system ailure, or disaster.

A. To permit timely restoration of information and business processes, should such events occur.
B. To manage and secure backup and restoration processes and the media employed in the process.
C. The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.
D. Backup retention periods are in contrast to retention periods defined by legal or business requirements.

▸ System Backup are not meant for the following purpose

1. Archiving data for future reference.
2. Maintaining a versioned history of data.

▸ Policy

Systems will be backed up according to the schedule mantling by the vendor **Millennium Medical System**.

Data stored on the desktop computers are regularly backed up as follows:

1. Incremental backup daily (**Mon.-Fri.)** and data located on-site.
2. Full backup weekly (**Sat.**) and data located off-site.

.

▸ Data Recovery

1. In the event of a catastrophic system failure, off-site backed up data will be made available to users within **2** working days if the destroyed equipment has been replaced by that time.
2. In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

▸ Restoration Requests

1. In the event of accidental deletion or corruption of information, requests for restoration of information will be made to **Executive Director.**

▸ Responsibilities

• Backups and Date Recovery By Technical Officer, @ **405 415-6039**

▸ 5a) Assertive technology

Assertive technology is provided to consumers and staff as long as it is a reasonable accommodation.

▸ Disaster Recovery Preparadness

⇥ Purpose and Scope Introduction

FOHFS Agency has set up a highly computerized operational environment. This includes the use of microcomputers in offices as well as servers that provide much of the operational support. Our office network ties these various computers together and provides communications to many computer networks, within and out **FOHFS Agency**. The reliability of computers and computer based systems has increased dramatically. Computer failures that do occur are normally diagnosed and repaired promptly using local IT contracted staff. Many computer systems contain redundant parts, which improve their reliability and provide continual operation when some failures occur.

▸ Objectives/Constraints

The major objective of disaster recovery preparedness is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction or minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting **FOHFS Agency** technology. Special attention and emphasis is given to an orderly recovery and resumption of those operations that affect the critical running of the **FOHFS Agency**, such as providing support to therapist. The Agency provides recovery within a reasonable amount of time and within cost constraints. The objectives of this disaster recovery preparedness plan are designed to provide support to **FOHFS Agency** therapist, support staff and Clients**.**

The senior staff member on site at the time of the incident or the first one on site following an incident will contact the **Executive Director** for a determination. The **Executive Director** will determine who else needs to be notified including when to notify out side vendors. The senior technology staff member on site at the time of the incident will assume immediate responsibility.

▸ Technology Resources Use Policy

Policy restricting personal use of employer's computers and systems

1. PURPOSE

- **a)** To remain competitive, better serve our customers and provide our employees with the best tools to do their jobs, **FOHFS Agency** makes available to our workforce access to one or more forms of electronic media and services, including but not limited to: computers, software, printers, copiers, files, databases, cellular phone, pager, email, telephones, voicemail, fax machines, external electronic bulletin boards, wire services, online services, intranet, Internet and the **World Wide Web**.
- **b)** **FOHFS** Agency encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information about vendors, customers, technology, and new products and services.

c) However, all employees and everyone connected with the organization should remember that electronic media and services provided by **FOHFS Agency** are Agency property and their purpose is to facilitate and support **FOHFS Agency** business.

d) All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

e) To ensure that all employees are responsible, the following guidelines have been established for using email and the Internet.

f) No policy can lay down rules to cover every possible situation. Instead, it is designed to express **FOHFS Agency** philosophy and set forth general principles when using electronic media and services.

Security

2. AUTHORIZATION

Access to the **FOHFS Agency** technology resources is within the sole discretion of the **Agency**. Generally, employees are given access to the Agency various technologies based on their job functions. Only employees whose job performance will benefit from the use of the Agency technology resources will be given access to the necessary technology. Additionally, employees must successfully complete Agency-approved training before being given access to **FOHFS Agency** technology resources.

3. PROHIBITED COMMUNICATIONS

Electronic media cannot be used for knowingly copying, transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene, sexually explicit, pornographic, defamatory or threatening;
- In violation of any license governing the use of software;
- Engaged in for any purpose that is illegal or contrary to **FOHFS Agency** policy or in a manner contrary to the best interests of **FOHFS Agency**, in any way that discloses confidential or proprietary information of **FOHFS Agency** or third parties, or for personal or pecuniary gain; or
- Protected by copyrights laws unless the employee has the author's permission or is accessing a single copy only for the employee's reference.

4. PROFESSIONAL CONSIDERATIONS

It is important to maintain a proper spirit and tone to your communications over the system. The following guidelines are suggested**:**

- Make your communications positive, constructive, complete, factual.
- Don’t write when angry and edit before sending.
- Be careful with humor – they can’t see you wink.

- ❑ Always avoid sarcastic humor.
- ❑ Never use all caps – that is perceived as "**SHOUTING**."
- ❑ Avoid belaboring disagreements in email – there is a time for face-to-face meetings.
- ❑ Always guide your recipient in responding by stating what you need and by when.
- ❑ Pay attention to grammar and spelling, both to protect your own reputation and intelligence, and to avoid irritating your recipients who are distracted by careless mistakes.

5. PERSONAL USE

The computers, electronic media and services provided by **FOHFS** Agency are primarily for business use to assist employees in the performance of their jobs. As long as personal use does not interfere with the employee's duties, is not done for pecuniary gain, does not conflict with **FOHFS Agency** business, and does not violate any **FOHFS Agency** policy, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes.

However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege. **FOHFS Agency** assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over or stored on **FOHFS Agency** technology resources. **FOHFS Agency** accepts no responsibility or liability for the loss or non-delivery of any personal electronic mail or voicemail communications or any personal data stored on any **FOHFS Agency** property. **FOHFS Agency** strongly discourages employees from storing any personal data on any of the Agency technology resources.

6. ACCESS TO EMPLOYEE COMMUNICATIONS

a) Generally, electronic information created and/or communicated by an employee using email, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and bulletin board system access, and similar electronic media is not reviewed by **FOHFS Agency.** However, the following conditions should be noted:

FOHFS Agency does routinely gather logs for most electronic activities or monitor employee communications directly, be it:

i) **Telephone Use and Voicemail:** Records are kept of all calls made from and to a given telephone extension. Although voicemail is password protected, an authorized administrator can reset the password and listen to voicemail messages.

ii) **Electronic Mail:** Electronic mail is backed-up and archived. Although electronic mail is password protected, an authorized administrator can reset the password and read electronic mail.

iii) **Desktop Facsimile Use:** Copies of all facsimile transmissions sent and received are maintained in the facsimile server.

iv) **Document Use:** Each document stored on **FOHFS Agency** computers has a history, which shows which users have accessed the document for any purpose.

v) **Internet Use:** Internet sites visited, the number of times visited, and the total time connected to each site is recorded and periodically monitored.

FOHFS Agency reserves the right, at its discretion and without notice, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other **FOHFS Agency** policies, or to investigate misconduct, to locate information, or for any other business purpose.

b) Employees should understand, therefore, that they have no right of privacy with respect to any messages or information created or maintained on **FOHFS Agency** technology resources, including personal information or messages.

c) Accordingly, if they have sensitive information to transmit, they should use other means.

d) All messages sent and received, including personal messages, and all data and information stored on the Agency electronic-mail system, voicemail system, or computer systems are Agency property regardless of the content. As such, the **FOHFS Agency** reserves the right to access all of its technology resources including its computers, voicemail, and electronic-mail systems, at any time, in its sole discretion.

e) Passwords do not confer any right of privacy upon any employee of **FOHFS Agency**. Employees are expected to maintain their passwords as confidential. Employees must not share passwords and must not access coworkers' systems without express authorization.

f) Deleting or erasing information, documents, or messages maintained on the **FOHFS Agency** technology resources is, in most cases, ineffective.

g) All employees should understand that any information kept on **FOHFS Agency** technology resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by an employee.

h) Because the **FOHFS Agency** periodically backs-up all files and messages, and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased.

i) Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential.

▸THE INTERNET AND ON-LINE SERVICES

FOHFS Agency provides authorized employees access to on-line services such as the Internet. The Agency expects that employees will use these services in a responsible way and for business-related purposes only. Under no circumstances are employees permitted to use the Agency Technology Resources to access, download, or contribute to the following:

- ❑ Gross, indecent, or sexually-oriented materials;
- ❑ Sports sites;
- ❑ Job-search sites;
- ❑ Entertainment sites;
- ❑ Gambling sites;
- ❑ Games, humor;
- ❑ Illegal drug-oriented sites;
- ❑ Personal pages of individuals; and
- ❑ Politically-oriented sites or sites devoted to influencing the course of legislation or public policy.

Additionally, employees must not sign "guest books" at Websites or post messages to Internet news groups or discussion groups at Websites. These actions will generate junk electronic mail and may expose the Agency to liability or unwanted attention because of comments that employees may make. The Agency strongly encourages employees who wish to access the Internet for non-work-related activities to get their own personal Internet access accounts.

▸ PARTICIPATION IN ONLINE FORUMS

j) Employees should remember that any messages or information sent on Agency-provided facilities to one or more individuals via an electronic network – for example, Internet mailing lists, bulletin boards, and online services – are statements identifiable and attributable to **FOHFS Agency.**

k) **FOHFS AGENCY** recognizes that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a news group devoted to the technical area.

Virus protection

▸ SOFTWARE

To prevent computer viruses from being transmitted through the Agency computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Only software registered through **FOHFS Agency** may be downloaded. No employee may load any software on the Agency computers, by any means of transmission, unless authorized in advance by **FOHFS Agency** system administrator. Only the **FOHFS Agency** IT person can download software on **FOHFS Agency**' computers. The computers are password protected, plus they are protected by Open **DUNS**, which restrict access to many Internet sites.

▸ Confidentiality

SECURITY/APPROPRIATE USE

l) Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by Agency management, employees are prohibited from engaging in, or attempting to engage in:

- ❑ Monitoring or intercepting the files or electronic communications of other employees or third parties;
- ❑ Hacking or obtaining access to systems or accounts they are not authorized to use;
- ❑ Using other people's log-ins or passwords; and
- ❑ Breaching, testing, or monitoring computer or network security measures.

m) No email or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

n) Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

o) Anyone obtaining electronic assess to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

p) The Agency has installed a variety of programs and devices to ensure the safety and security of the Agency technology resources. Any employee found tampering or disabling any of the Agency security devices will be subject to discipline up to and including termination.

▸ ENCRYPTION

Employees can use encryption software supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a Agency computer must provide their supervisor

with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

▸ CONFIDENTIAL INFORMATION

FOHFS Agency is very sensitive to the issue of protection of trade secrets and other confidential and proprietary information of both the Agency and third parties ("Confidential Information"). Therefore, employees are expected to use good judgment and to adhere to the highest ethical standards when using or transmitting Confidential Information on the Agency technology resources.

Confidential Information should not be accessed through the Agency technology resources in the presence of unauthorized individuals. Similarly, Confidential Information should not be left visible or unattended. Moreover, any Confidential Information transmitted via technology resources should be marked with the following confidentiality legend:

"This message contains confidential information. Unless you are the addressee (or authorized to receive for the addressee), you may not copy, use, or distribute this information. If you have received this message in error, please advice FOHFS AGENCY immediately at 405-735-3716 or returns it promptly by mail."

▸ VIOLATIONS

Any employee who abuses the privilege of their access to email or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

▸ PROCEDURES

Procedures for accessing the Voicemail, Email and Internet system, as well as the guidelines for how to properly send and retain information, may be obtained by contacting **TECHNICAL/COMPLIANCE OFFICER**. Each employee on a semi-annual basis is required to review the Voicemail/Email/Internet policies and procedures. Questions concerning the use of the Voicemail/Email/Internet system should be directed to the systems administrator. Questions concerning the improper use of the system should be directed to the employee's immediate supervisor, and if not satisfied with the response, to the systems administrator.

Fountain **o**f **H**ope **F**amily **S**ervice **I**nc.
10326 Greenbriar Parkway
Oklahoma City, Ok 73159

End User Information System Access Request

Employee Name_____ **EmpID**_____

Email _____Phone_____

DeptID _____DeptName_____

Position /Job Function _____

DeptID Requesting Access To_____ _____

Requestor Agreement

By signing this form, I certify that I have read and understand the statement of confidentiality of records. I understand that my **FOHFS ID** and password are to be kept confidential. Should I share this information, my access will be revoked.

Requestor Signature _____**Date Signed**_____/_____/20_____

Manager Approval (Only)

By signing this form, I approve this employee for access requested on the following pages, including access to confidential student and/or employee data.

Manager Approval_____**Date Signed**____/_____/**20**_____

Manager Name_____**Manager Phone ( ) -**

Manager Email_____

Access Request –Check Requested Items

Access will only be granted if the proper training courses have been completed, and the functionality is required to perform your job. The **FOHFS** Training Team, in conjunction with the Finance, Human Resources, Inter Students. Information Security Officer has the final signoff on the access that should be granted.

____Accounting ____HR _____Clinical _____Reports _____Query _____Web Site ____Email