

**South Florida Behavioral Health Network, Inc.**

**Information Technologies Policies and Procedures Manual**

**Version 4**

**July 2010**

# Table of Contents

[Table of Contents 2](#_bookmark0)

[Information Technology (IT): Overview 3](#_bookmark1)

[User Access 4](#_bookmark2)

[Password Management 5](#_bookmark3)

[Software Installation and Management 7](#_bookmark4)

[Saving User Data to Server 9](#_bookmark5)

[HIPAA Compliance 10](#_bookmark6)

[Security Incident and Response Reporting 11](#_bookmark7)

[PC Security and Virus/Adware Protection 12](#_bookmark8)

[Laptop Security 12](#_bookmark9)

[Server Security 12](#_bookmark10)

[Virus and Adware Protection 12](#_bookmark11)

[Data Storage, Backup and Data Backup Storage 13](#_bookmark12)

[Data Storage 13](#_bookmark13)

[Data Backup 13](#_bookmark14)

[Data Backup Storage 13](#_bookmark15)

[Troubleshooting and Maintenance 14](#_bookmark16)

1. [mail/Internet Access, Acceptable Use and Security 15](#_bookmark17)
   1. [mail and Internet Access 15](#_bookmark18)

[Acceptable Use 15](#_bookmark19)

[Internet Security 15](#_bookmark20)

* + - The purpose of this Information Technology (“IT”) policy and procedures is to establish guidelines for the use and management of IT equipment (workstations, servers, printers, etc.) by the South Florida Behavioral Health Network (SFBHN) and for the implementation of a level of security which will provide for the protection of data and information technology resources from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside the company.
    - The procedures listed in this document establish the methods SFBHN will use to protect the confidentiality, integrity, availability, and reliability of all information technology resources used to support the needs of our clients and the mission of the agency.
    - This policy applies to all employees of SFBHN, to non-SFBHN staff performing work on behalf of SFBHN, and to all IT resources whether owned, leased, or contracted by SFBHN.
    - SFBHN’s IT Security Officer is responsible for implementing and monitoring the procedures described in this document.
    - The IT department may purchase or lease and install software to monitor or enforce the policies and procedures described herein.

Access to SFBHN’s servers and system resources by SFBHN or outside sources will be determined by the IT Security Officer in coordination with the Executive Director and the department heads. Existing federal and state regulations (such as CFR-42 and HIPAA) and each staff’s position requirements will be taken into consideration in determining the staff’s level of access.

* + - An electronic log will be kept listing those individuals that have access and a list of the authorizations they have been granted.

The following policies apply regarding user accounts and passwords:

* + - In order to have access to the company’s IT resources (e-mail, servers, workstations, printers) all users must obtain a user account from the SFBHN’s IT Security Officer. Once the accounts are established, users will set their own passwords to gain access to those resources.
    - Passwords are required for the network account, e-mail account, access to the main client database and any other account the user may be assigned to. Although this is not a requirement, preferably each account should have a different password.
    - Unless specifically indicated otherwise, passwords are established by each user, and should not be disclosed to anyone, including the user’s supervisors or the network administrator. This rule clearly does not apply in the case of accounts administered by external sources, where passwords may be set by a third party.
    - Passwords should not be written down, much less posted in an insecure location (such as on a computer monitor).
    - The network administrator, depending on the technology used, can set specific rules for the construction of passwords (such as: minimum or maximum number of characters in the password, whether the password must contain a combination of alphabetic, numeric and special characters, whether passwords are case-sensi- tive, etc.).
    - Passwords should never be easy to guess by other staff members. As examples of easy-to-guess passwords: the user ID, the user’s name, the name of a pet or a family member, the user’s date of birth, etc.
    - The network administrator may enforce additional rules such as passwords being changed on a regular basis (e.g., every 90 days), or passwords to be unique (i.e., once a password has been used, it can never be used again.).
    - Should the IT department ever need to open the sealed envelope containing a user’s set of passwords, the user, his or her supervisor, the network administrator, the Executive Director and the Deputy Director/Chief Financial Officer should be notified of this fact as soon

as possible. In this case, the old passwords will be invalidated and the user should immediately establish a new set of passwords.

* + - If there are reasons to suspect a password has been compromised, the network administrator has the authority to disable an account or change a user’s passwords, temporarily suspending user access to the account(s). In such cases, the Executive Director, the Deputy Director/Chief Financial Officer, the user’s supervisor and the user will be notified as soon as possible.

# Software Installation and Management

* + - It is SFBHN’s policy that the members of the IT department are the only persons authorized to install, update or remove software from a workstation, to add or remove printers or, in general, to change workstation settings. On a case by case basis, other staff members may be authorized by the network administrator to perform these tasks.
    - It is SFBHN’s policy to ensure that all software installed in computers property of the company is either in the public domain or has been legally purchased or leased by the company.
    - It is SFBHN’s policy that any software found installed on a workstation which violates the policies stated in this section will be immediately deleted upon detection.
    - The IT department will assign each server, workstation, laptop or notebook an administrator password that will be known only to the members of the department.
    - The IT department will then establish user profiles in order to protect the programs and data in a workstation from being accidentally or intentionally deleted by users, prevent the installation of non- authorized or conflicting software, prevent users from saving information to specified locations, prevent the access, installation or removal of printers and other hardware and, in general, prevent users from changing a workstation’s configuration.
    - IT department staff are the only persons authorized to install, update or remove software from servers and workstations, to add or delete printers and, in general, to change workstation settings.
    - IT department staff will review periodically the software installed in company workstations to ensure that all the software has been legally purchased or leased by SFBHN.
    - The IT department will keep a log of installed software to make sure that the number of licenses purchased or leased is not exceeded.
    - Any software found that doesn’t meet the above requirements will be immediately deleted. The IT department will keep a log detailing the workstation ID, the staff assigned to the workstation, the name of the software, and the dates of discovery and removal.
    - If it is determined that a staff member has violated company policy by installing illegal or unauthorized software, this fact will be reported immediately to the network administrator, the staff’s supervisor, the Deputy Director/Chief Financial Officer and the Executive Director - who will decide the appropriate course of action.
    - Each member of SFBHN staff will be assigned a specific network drive to store their work. Users will be made aware that they must save their documents only to their designated network drives. In particular, no client protected information should ever be stored in diskettes or other removable media.
    - In the case where several users need common access to some files, the IT department will create special shared network folders for that purpose.
    - In accordance with current federal regulations (HIPAA), it is SFBHN’s policy to make sure that no client protected information is electronically stored in a location where it can be read or accessed by non authorized users who may have physical access to workstations. If the client’s information is stored in a workstation’s local hard drive, individual profiles will be maintained in the workstation so that only authorized staff using the workstation will have access to the information.
    - In accordance with SFBHN’s IT policy on HIPAA compliance, it is SFBHN’s policy to ensure that no client protected information is electronically submitted unnecessarily.
    - Should client information need to be transmitted, information will be password protected before being sent. The password is then sent as part of a separate email and/or the person is notified of password verbally through a phone call.
    - Confidentiality Notices such as the following will be included on all email transmittals:

“This message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information that is exempt from public disclosure. Any unauthorized review, use, disclosure, or distribution is prohibited. If you received this message in error please contact the sender (by phone or reply electronic mail) and destroy all copies of the original message.”

* + - Should client information be unintentionally transmitted by an SFBHN staff member, SFBHN’s IT Department will be made aware of security breach.
    - Should client information be intentionally transmitted by SFBHN staff member, staff member will be disciplined as outlined in SFBHN’s Human Resources policies and procedures.
    - All security incidents will be tracked by SFBHN’s IT Department and will subsequently generate reports as requested by Executive Management regardless of transmittal type.

# Laptop Security

* + - To provide security against the loss of portable equipment, it is SFBHN’s policy to provide all laptops and notebooks with a “boot password” required for the computer to start. The boot password will be known only to the IT department and the unit’s designated user(s).

# Server Security

* + - Servers are vital to a network, since they provide access to data and resources such as modems, routers and printers. Special measures are needed when a server is accessible over the Internet, since it can then become accessible to users outside the company’s intranet.
    - It is SFBHN’s policy that all company servers will be placed in a secure location, such as in a locked room with restricted access. In cases when it is not possible to place a server in a locked room, it will be placed in a lockable case, ensuring that the case is always locked.
    - It is also SFBHN’s policy to provide additional server and workstation security by a combination of firewalls and anti-virus software.

# Virus and Adware Protection

* + - All servers and workstations property of SFBHN will have anti-virus and adware removal software installed at all times so that all data input to the system is constantly monitored. IT staff will periodically verify through the product’s monitoring tools the virus-free status of each system.
    - In addition, daily virus scans will be scheduled to run off hours or at the time the workstation is turned on.

# Data Storage

* + - Each computer user will be provided with a personal folder in one of the company’s servers to store all their files. Users will be advised to save their files only to their designated network drives.
    - If several users need common access to specific files, the IT department staff will create special folders for that purpose and implement the corresponding access rights.

# Data Backup

* + - It is SFBHN’s policy to protect the information contained in its servers by means of periodic tape backups. Backups are normally scheduled to run at the end of the day during non-working hours.
    - Enough tapes will be kept to maintain a two-week daily backup cycle (Monday through Friday), plus at least six additional monthly backups and a full system backup at the end of each fiscal year.
    - Daily backups will be overwritten at the end of the ten-day cycle. Monthly backups will be overwritten after six months and yearly backups will be kept for seven years.
    - An electronic backup log will be maintained by the backup software.

# Data Backup Storage

* + - To guarantee that backup tapes are not destroyed along with the server(s) in case of a natural disaster tapes will be stored at an outside location to be determined by the Executive Director and the network administrator. Both officers will also determine a method for tape collection and retrieval.
    - The IT department performs periodic inspection of company hardware with the purpose of detecting potential problems and to perform such tasks as scheduled maintenance and software updates.
    - SFBHN will perform routine maintenance on its equipment at least twice a year. Maintenance will include tasks such as system checkups, hard drive checks, deletion of temporary and Internet cache files, hard drive defragmentation and installation of software updates and patches.
    - In addition, all company servers, workstations and laptops or notebooks will be programmed to automatically upload and install critical updates and security patches.
    - The schedule for such maintenance will be determined by the IT department.
    - An electronic log will be kept of such maintenance.
    - Whenever possible, IT staff will try to perform maintenance tasks off regular hours in order not to interfere with regular equipment use. SFBHN staff may be instructed to leave their workstations on in order to be remotely accessed by the IT staff when such maintenance is required.

# mail and Internet Access

* + It is SFBHN’s policy that both Internet access from SFBHN property and corporate e-mail should be used exclusively for work-related purposes, and that neither can be used in a way which is offensive to an individual or a group of individuals.
  + In order to guarantee the above, both Internet access and the use of company e-mail can be monitored by the IT staff.

# Acceptable Use

* + All employees will be assigned an electronic mail account, which will be used to receive and send e-mail, both interoffice and external.
  + Employees should use the company’s e-mail program exclusively for sending company mail.
  + Employees will be made aware that the company may be liable for any e-mail originating out of its corporate account. Therefore an “acceptable use policy” will be implemented in a separate document.
  + Employees will be made aware that the company reserves the right to monitor e-mail use by its staff.

# Internet Security

* + In order to provide maximum security all access in and out of the company’s intranet will be made through a single router performing network address translation (NAT) through a firewall. That provides for a single point of access and control.
  + The router will be programmed to block all ports not required by company’s operations.
  + Employees will be made aware that the company may monitor Internet access at any time.