Anderson-Oconee-Pickens Mental Health Center
Information Technology Plan

Updated 2/2021

AOP is committed to the innovative use of technology to improve our efficiency and promote a better built environment. Our priority is provide day-to-day smooth operations and technological solutions.

GOALS/PRIORITIES:

Our goal is to maintain and enhance the IT infrastructure to support the operations of the School Mental Health Counselors who provide services through VPN and staff who provide Community Services as well as On-Call services. This is accomplished by providing staff with DMH encrypted Laptops, Aircards and etokens. In the event of a technology related emergency while staff is providing services via telehealth, staff should notify the AOP helpdesk (aophelp@scdmh.org) or contact IT staff, Della Wideman, 965-9237 or Dustin Marchbanks, 965-9271.

Due to COVID-19, support will continue to be provided to staff, using Zoom, Doxy.me, and Teams remotely, working from home, or in the office and Telepsychiatry. Web cams for desktops will be provided to accommodate staff using these applications. Additionally, VDI (Virtual Desktop Infrastructure) will be put in place which creates a virtualized desktop environment on a remote server setup. Users will be able to access their desktops or laptops remotely through their devices from anywhere at any time through VDI. The user will be able to log into the same desktop each time. Security is another vital aspect of VDI. The OS (Operating System), Applications and some data are all stored on the local hardware like laptops or PC's. In case the computer is stolen or damaged, all the data is lost. With VDI, as remote data servers store that data, there will be no data loss. Even if the device is lost, users can still access their desktops virtually from any other device. The desktop or laptop is not bound to the hardware; it can be accessed from multiple devices.

Door Access System will be put in place in the next four years, which will allow DMH employees to access entrance to any DMH location using their ID badges. Surveillance must be stored for 30 days. The cost for each building will be about $25,000 initially after which there will be a charge of $1,000 annually for maintenance. This bill has not passed yet but is being processed. Badges will be changed to work with the system. Camera surveillance will also be required as a part of accreditation process, which will also be included in the next four-year plan.

WiFi is still an option for all locations. Currently C&A is the only location that has access. This will provide network connections for SMH Services, CBS, etc. and other staff that have laptops that otherwise would not be able to physically connect to the network. Timeframe for the other locations could be in the next 2-3 years, but first firewalls must be inspected to ensure locations are cleared for WiFi access. WiFi routers as well as WiFi switches will need to be in place to accommodate wireless connections.

POLICIES & PROCEDURES:

The Center and SCDMH has a comprehensive set of policies, procedures, and processes that ensure the operability, security and integrity of its computer system and data. These include the center IT Policies and Procedures, SCDMH IT Policies and Procedures, SCDMH Three Year Information Technology Plan, and the AOP Privacy Policy and the SCDMH Privacy directive. The following is a description of these policies, procedures, and processes. This IT Plan supports management and

is used for performance improvement activities such as making changes in program/service delivery and business functions.

1) Hardware/Replacement

The Center has established various maintenance contracts that ensure the replacement/repair of all of its computer equipment. PC's, Servers and printers are covered by The SU (Specialty Underwriters) Group with a 24 hour response time.

Routers and Switches are covered by ONIT with a 24 hour response time.

WAN Lines are serviced by AT&T.

2) Software

The Center maintains proper user licenses for all of its software, and replacement access if the original media is destroyed or inoperable. All software currently being used on the network conforms to the software requirements issued by Network Services

See below "SCDMH Division of Information Resource Management Policies and Procedures, Sub-Policy, Software Acquisition, Rev.2 06-07-00".

3.3.2 Software Acquisition Policy

Whether the technology (software and databases) used by DMH is owned by users or third parties and is protected by copyright and/ or other laws, or subject to license or other contractual agreements, it is the policy of DMH that users abide by any legal restrictions imposed by the owner of the technology (software and databases). The responsibility is imposed by the owner of the technology (software and databases) to make the nature of the restrictions known to the Director of ONIT.

The use of invasive software such as "worms" and "viruses" destructive to computer systems is unethical and illegal. Violations of copyrights and terms of license agreement are prohibited by law. Even when technology is not so protected, such violations are contrary to ethical behavior. Copies of software should only be made with proper ONIT authorization. Ignorance of the law is not a defense in court when employees steal an asset or personally benefit from it.

Computer users using DMH technology will be personally and solely responsible and liable for illegal activities. The State of South Carolina will be relieved of any legal responsibility.

See below AOP MHC Center Policy # 10-01-02 "Unauthorized Use of Data Media (software)".

POLICY:
It is the policy of Anderson-Oconee-Pickens Mental Health Center that there shall be no unauthorized use of software or Data Media (diskettes or CDs) on any of its computer systems.

PROCEDURE:
All Data Media/Software used on AOP's computer system must be licensed and/or registered with the manufacturer of that Data Media/Software. Furthermore, Anderson-Oconee-Pickens Mental Health Center shall maintain a log of these licenses

and Data Media packages used and installed on its computer systems. All Data Media must be submitted to the Computer Services and Quality Improvement Department for prior authorization and use and placement in the Data Media/Software log.

Security/Confidentiality

The Center ensures data security/confidentiality through monitoring and limiting physical access to File Servers, printers, fax machines, and PCs, and requiring unique USER ID's and confidential Passwords and 5-minute screen saver lock-outs.

The Center's Network is protected by the State Firewall, which restricts access to unauthorized Users. In addition, based on their job duties, individual users only have access to those data elements that are required for them to perform their duties. Any outside connections to our network can be access by logging on to VPN (Virtual Private Network) and using their 2-Factor Authentication token to access the internet at the user's location assigned them, such as the school districts, jail, etc. VPN is accessible using aircards that have been provide for each user, and/or home ISP's and tokens/MFA on their mobile devices, which is essential to access the Virtual Private Network (VPN).

Confidentiality is also guided by the DMH Directive # 837-03 "Privacy Practices".

Security is also guided by AOP MHC Policy # 10-01-01 "Electronic Data Security".

All staff is required to complete and pass the HIPAA 3 security module through Pathlore's Learning Management System for DMH. Users sending any HIPAA protected information outside DMH must encrypt information using encryption software provided.

AOP MHC adheres to the following SCDMH security guidelines stipulated in SCDMH Division of Information Resource Management Policies and Procedures, Rev. 2 06-07-00.

1. *Use only the DIRM approved versions of systems software, client software and patches.*
2. *Check regularly for viruses.*
3. *Localize File Server in a secure room and/or enclosure.*
4. *Select "Lock File Server Console" from the monitor main menu when the Microsoft console is not in use.*
5. *Limit the number of users with Admin rights.*
6. *Use access control Windows Active Directory to limit users to necessary applications and data.*
7. *Enable intruder detection and lockout.*
8. *Advise users to log out when their workstations are unattended.*

9. *Secure unattended workstations.*

10. *Require passwords of at least eight characters on all accounts.*

11. *Force passwords change every three months.*

12. *Require unique passwords.*

13. *Limit the number of grace logins at password expiration.*

3) Virus Protection

The computer network is protected from viruses through various means. The main protection is Windows Defender, which runs continuously on all PCs/Servers on or off the network. In addition Sandblast has been put in place to protect the network from sophisticated attacks and zero-day threats.

In addition, the AOP Policy "Unauthorized Use of Data Media/Software" restricts the introduction of all out-side media to the network, unless there is prior authorization, license registration, and virus scan by the center IT Services.

4) Assistive Technology

The Center offers Telepsychiatry (I.P.-based), electronic forms, a Center and SCDMH internet informational Website, a Center and SCDMH Informational intranet Website, including online learning modules, and means of assisting staff through technology. The array of assistive technology has expanded, including speech recognition (Dragon Naturally Speaking), Electronic Medical Records (EMR), and web-based services.

To prepare for a non-technology related emergency, all staff providing telepsychiatry should become familiar with the emergency procedures of the remote site, if they exist. The staff is also required to be prepared with local emergency resources and contact numbers to be provided to a patient should an emergency arise.

5) Backup Policy

See Below, Tape Backups, Policy # 10-01-03

Policy:
It is the policy of Anderson-Oconee-Pickens Mental Health Center to perform daily backups on each File Server to ensure data recovery.

Procedure:
There is only one server for four locations. Backups are to be performed daily on the main file Server at the Anderson Center and rotated off-site using Veritas Backup Exec. The Daily tape is utilized Monday-Thursday, Weekly tape is rotated on Fridays, and the Monthly tape is rotated the last Friday of each month. The monthly tape will be rotated off-site to the IT Department location.

Backup tapes are stored in a locked cabinet, apart from the main server location. Recovery/Restore tests will be performed quarterly to ensure recovery of data is restored appropriately.

6) Disaster Recovery Preparedness

Disaster Prevention/Recovery incorporates the following items: hardware maintenance, server security, site security and backup storage procedures.

1. *File Servers and Routers must have maintenance agreements. It is recommended that switches and concentrators also have maintenance agreements. File Servers, Routers and switches should be on a UPS (Uninterruptible Power Supply) to protect the equipment from power damage.*

2. *Backups are to be done daily on the File Server and rotated off-site. Rotations must be set-up with a satellite building. Daily rotation is the preferred standard with a required weekly minimum.*

3. *The File Server is password protected and is required to remain password locked at all times except when being accessed for maintenance by ONIT. Supervisor passwords will be limited to authorized personnel only.*

4. *Physical access to the File Server's operational area will be restricted unless it is under the close and immediate supervision of the Systems Administrator (SA).*

5. *Complete restoration of the File Server should be coordinated with the ONIT in Columbia prior to any restoration.*

6. *Local SAs should use all Network Security features and protective measures to keep their network data secure. The following security guidelines are suggested as a minimum:*
   - *a. Use only the ONIT approved versions of systems software, client software and patches.*
   - *b. Check regularly for viruses.*
   - *c. Locate File Server in a secure room.*
   - *d. Select "Log off User" from Start, Shutdown menu when the File server console is not in use.*
   - *e. Limit the number of users with SUPERVISOR rights.*
   - *f. Enable intruder detection and lockout.*
   - *g. Advise users to log out when their workstations are unattended.*
   - *h. Secure unattended workstations.*
   - *i. Require passwords of a least eight characters on all accounts.*
   - *j. Force passwords to change every three months.*
   - *k. Require unique passwords.*
   - *l. Limit the number of grace logins at password expiration.*
   - *m. Limit concurrent connections*

8) TELEPSYCHIATRY

Telepsychiatry services is provided for clients when face-to-face services are not available. Staff who delivers services will be trained on equipment to include, features, setup, use, maintenance, safety considerations, infection control and troubleshooting.

Clients will not having any contact with the equipment. Prior to the start of each session, all participants in the session are identified, including those at the originating site and remote site.

9) AUDIO, VIDEO RECORDINGS AND PHOTOGRAPHING

There are no audio or video recordings on patients served, however, photograph of patients are being done to identify each patient which is a part of their Electronic Medical Record (EMR). There will be provisions in the future to add Audio and Video recordings.