SANILAC COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY

NUMBER: BA013

NAME: IT SECURITY POLICY

INITIAL APPROVAL DATE:	01/09/2008	BY: Administrative Committee
(LAST) REVISION DATE:	08/31/2023	BY: CIO
(LAST) REVIEW DATE:	09/21/2023	BY: Policy Committee
DISCONTINUED DATE:	N/A	REPLACED BY: N/A

I. PURPOSE

Sanilac CMH has adopted this policy on IT Security to comply with HIPAA, with the regulation requirements for such a policy, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of Sanilac CMH must be familiar with the contents of this policy and follow its guidance, as appropriate. Familiarity with the plan and demonstrated competence in the requirements of the plan are an important part of every Sanilac CMH employee's responsibility.

II. APPLICATION

Populations: **ALL**
Programs: **Direct - ALL**
Contracted - ALL

III. POLICY

The Sanilac County Community Mental Health Authority (Sanilac CMH) computing and communication resources are intended for Sanilac CMH business purposes and for professional growth through the sharing of information and ideas. It is expected that use of the Sanilac CMH computing and communication resources will follow security guidelines put into place by HIPAA, HITECH, federal/state regulations, contract requirements, our accreditation body and specific definitions within this policy.

IV. STANDARDS

Sanilac CMH and its employees must protect the confidentiality and security for individuals we serve and the Agency's data resources. The following must be followed to insure the protection of data and resources. Use of the computer system, email, fax machines, printers, copiers, cell phones or any other data transmitting devices constitutes consent to this policy.

A. Computer monitors must not face doorways even if they have a privacy screen.
B. Computers must be password locked when the user is not present.
C. Passwords cannot be shared with anyone, written down, emailed, faxed, texted, or stored in an unsecured area. Passwords can be shared with IT Department staff; however, it must be shared in a secure manner.
D. Any new passwords must be a mix of letters and numbers; they must also have at least one capital letter and be at least 12 characters long.
E. Users cannot keep data on any portable media i.e., CD, DVD or USB Memory stick that is not encrypted and password protected, or otherwise safeguarded by the IT Department. Digital

Cameras are excluded. Any secure data that staff pass to and from Agency computers must use IT Department purchased encrypted USB Thumb drives and have approval from the CIO. Any special circumstance regarding data transfers must be approved by the CIO.

F. Staff are responsible for cell phone security. Cell phones must have a password for the phone and voicemail.
G. Any identifiable information about individuals we serve is prohibited from use over cellular voice devices; this includes Agency cell phones, unless an emergency is occurring or time sensitive information is necessary for the safety or immediate well-being of the individual.
H. Smart Phones that contain Agency data such as email messages must be password or biometrically protected and set to automatically lock the screen when not in use. Passwords must be at least 6 characters long. This applies to both Agency-owned and approved personal devices.
I. Staff are responsible for the security of all devices provided or paid for (even in part) by the Agency, such as laptop, computer, tablet, cellphone, smartphone and digital camera. This includes protection from theft and secure use in public areas. Staff must report a theft or breach of such device immediately to a supervisor and the IT Department.
J. Use of Agency email through smart phones is restricted to Agency Officers or staff designated by exception of the CEO and/or the CIO.
K. Email access from outside of the Agency using web mail is restricted to Agency Supervisors and Officers. Temporary exceptions for staff will be made by the CIO.
L. Confidential documents can't be left sitting on printers, scanners, fax machines or copiers.
M. Identifiable information regarding individuals we serve must not be emailed outside of the Agency network unless the message is encrypted. The staff member must follow the proper procedure for encryption.
N. Any information received unintentionally such as emails and faxes must be completely deleted and destroyed. This information must not be passed on. This must be reported to the IT Department.
O. Staff cannot work from home with non-agency equipment unless an exception is granted by the CEO or CIO.
P. Staff who work from home must complete forms 0556 and 0557
Q. Any device that connects to the Agency network, both wired and wireless (*excluding guest internet access*) must be inspected and approved by the IT Department.
R. Wireless connected devices including but not limited to, laptops, tablets and smartphones must be approved for use by the IT Department. Wireless access to the private staff network is password protected and all connected devices will be inventoried and tracked by the IT Department. Wireless passwords must not be shared or copied to unapproved wireless devices.
S. Guest wireless access for the public and personal staff devices is provided via a password protected and segregated internet-only wireless network. The IT Department will not keep an approved device list for this network; however it will be monitored. The IT Department can and will remove access to devices on this network if deemed necessary by the CEO and/or CIO.
T. Any approved device connected to the Agency network must have current and updated antivirus software unless connected through the guest wireless network.
U. Wireless access for both public/guest use and private/protected staff use will be secured with passwords. Private access will only be granted by the IT Department staff on approved devices. Only IT Department staff will have access to the private network password, and it will not be given out to staff. This password must be categorized as a complex password. Both public and private access will be monitored, and when deemed necessary, passwords will be changed without notice by IT Department staff.

V. **DEFINITIONS** – None.

VI. ENFORCEMENT

All Supervisors are responsible for enforcing this policy. The IT Department, HIPAA Officer and Security Officer will perform audits and enforcement. Employees who violate this policy are subject to discipline up to and including termination from employment, professional discipline, or criminal prosecution in accordance with the facility's Sanction Policy.

VII. ATTACHMENTS

VIII. REFERENCES

- Form 0556 – Telecommuting Agreement
- Form 0557 – Telecommuting Location Safety Checklist