SANILAC COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY

NUMBER: BA038

NAME: ACCEPTABLE USE POLICY

INITIAL APPROVAL DATE:	07/18/2001	BY: Administrative Committee
(LAST) REVISION DATE:	07/26/2023	BY: CIO
(LAST) REVIEW DATE:	06/20/2024	BY: Policy Committee
DISCONTINUED DATE:	N/A	REPLACED BY: N/A

I. PURPOSE

Sanilac CMH has adopted this policy on Acceptable Use to comply with HIPAA, with the draft 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, and all facility personnel that use electronic devices (i.e., computers, laptops, smart phones, etc.), must be familiar with the contents of this policy and follow its guidance, as appropriate, when using Agency equipment. Familiarity with the plan and demonstrated competence in the requirements of the plan are an important part of every Sanilac CMH employee’s responsibility, as well as that of every other facility employee who uses Agency equipment.

II. APPLICATION

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

III. POLICY

The 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 Sanilac CMH computing and communication resources will fall within the guidelines of generally accepted social and business standards and demonstrate respect for all individuals. The employees’ devices are to assist Sanilac CMH in conducting day-to-day business.

IV. DEFINITIONS

None

V. STANDARDS

Sanilac CMH encourages the business use of devices to increase productivity. The devices and all data and software generated by or handled by the devices, including back-up copies, are part of the business equipment of Sanilac CMH, are owned by the facility, and are not the property of the users of the system. Consequently, device users do not have a right to privacy in their use of the Agency systems or its data storage component. Sanilac CMH reserves the right to monitor, audit, delete and read data created by usage of the Agency systems. The IT Department may override user passwords. The IT Department will determine and delete if needed, any non-pertinent files such as, but not limited to, temporary files and cache files. Any other type of files that the IT Department deems unnecessary will be discussed with staff and/or their supervisor before deletion. Although it is the policy of Sanilac

CMH not to regularly monitor the contents of devices or the data created by an employee, it may monitor the contents and usage to support operational, maintenance, auditing, security and investigative activities. Users should use their devices and the computer system with the knowledge that Sanilac CMH may from time to time examine the content of devices and data created by usage of the computer system. Nor can Sanilac CMH guarantee that any device information and data created by usage of the computer system will be private. Use of the computer system constitutes consent to this policy.

Generally, computer and phone users should restrict their use of the systems to proper business purposes relating to the care and treatment of individuals we serve and related administrative matters, such as billing. A user may, however, use the computer system for personal purposes, under the following conditions:

A. Personal use does not involve significant use of the facility’s resources, such as work time, computer time, costs and the like, and does not preempt any business activity or interfere with the user’s or other’s productivity.

B. All computer users will monitor the computer’s operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system.

C. Users may not alter settings or configurations preset on their devices. Users will complete a Track-It Work Order or contact the Help Desk when requesting work to be completed on a device.

D. Only Sanilac CMH owned or authorized software and hardware installed by the IT Department are to be used with the devices. If software or hardware presented to the IT Department for approval is denied, and the staff member is persistent regarding the validity of the request, the request will be brought to CIO/Admin Committee for review.

E. All computers plugged into an electrical power outlet will use a surge suppressor approved and installed by the IT Department. No other electrical equipment, for example, radios, CD players, calculators, coffee makers, etc. shall be plugged into the same surge suppressor as the computer equipment. Plugging of electric heaters is prohibited in the same electrical outlet as computer equipment surge suppressors.

F. All personnel using computers will familiarize themselves with and comply with the facility’s disaster plans and take appropriate measures to protect computers and data from disasters.

G. All new employees who will be using the computer equipment will be given a Sanilac CMH computer system and applicable software and be trained on common computer system functions by the IT Department.

STANDARDS cont.

H. Personnel logging onto the system will make a good faith effort to ensure that no one observes the entry of their password. Personnel will not log onto the system using another user's account. Nor will personnel enter data under another user's account. Users will not write any passwords down.

I. Each person using the facility's computers is responsible for the content of any data he or she inputs into the computer system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All personnel who utilize the system will familiarize themselves with and comply with the facility's Communications Policy, and the IT Security Policy.

J. No employees may access any confidential protected health or operational information that they do not have a need to know. No employee may disclose confidential information regarding individuals we serve unless properly authorized to do so. All personnel should familiarize themselves with the Confidentiality and Disclosure of Information policy RR005.

K. Employees must not leave printers unattended when they are printing confidential documents or protected health information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer. Employees must comply with HIPAA guidelines to ensure confidentiality when utilizing any agency equipment.

L. Employees may not use the facility's system to solicit for outside business ventures, organizational campaigns, or political or religious causes. Nor may they enter, transmit, or maintain communications of a discriminatory or harassing nature or materials that are obscene or pornographic. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain or transmit any abusive, profane, or offensive language.

M. The use of a screen lock will be implemented by the IT Department staff so as to implement computer security that is needed for day-to-day business operations. To prevent an unauthorized user from viewing the information displayed on an employee's computer screen, the employee may shut off the monitor at any given time or lock the workstation. Employees must comply with HIPAA guidelines to ensure confidentiality when utilizing any agency equipment.

N. Each user must log off the system/enable screen lock if he or she leaves the computer terminal for any extended period of time.

O. To protect against the transmission of computer viruses into the facility's system, no personnel, except those authorized by the IT Department, will be allowed to utilize information from a CD or flash/portable drives that has been used by any computer other than those in our Agency running our anti-virus software. When documents are received or brought into the Agency, before they can be accessed by any staff, they must be scanned for viruses by a member of the IT Department or a staff member who has been trained by the IT Department.

P. Laptop computers and tablets pose a significant security risk because they may contain confidential protected health information and, being portable, are more at risk for loss, theft, or other unauthorized access than the facility's less easily movable computers.

Q. Sanilac CMH will issue to employees, with approval of their supervisor, checkout computer equipment on which they will be specially trained. The hardware, software, all related components, and data are the property of Sanilac CMH and must be safeguarded and returned upon request and upon termination of your employment. The employee is responsible for the security of the checkout computer equipment and software while they are in their use. The check-out equipment will be brought into the IT Department upon request for routine maintenance and upgrades as necessary.

R. User is not permitted to connect to any unauthorized services, such as Internet providers, Wi-Fi, or any other connection service in any manner without the approval of the IT Department. The user understands that the hardware has not been set up for any other usage other than those intended for completion of their business. Altering of these settings and configurations is expressly prohibited.

S. Computers, associated equipment and software are for business use only, not for the personal use of the user or any other person or entity. Users will not permit anyone else to use Agency devices for unapproved purposes, including but not limited to, the user's family, and/or associates, individuals we serve or their family.

T. Users will not upload/download any software onto devices except as loaded by the IT Department.

U. Users will not insert any CDs flash/portable drives or other media into the computer without the express authorization of the IT Department.

V. Users must use only batteries and power cables provided by Sanilac CMH. Users will not connect to any additional peripherals (keyboards, printers, modems, etc.) without the express authorization of the IT Department.

W. Users are responsible for securing the unit, all associated equipment, and all data within their homes, cars, and other locations. The devices will not be left unattended unless it is in a secured location. Users may not leave equipment in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.

X. Users must place devices and associated equipment in their proper carrying cases when transporting them. The case must display "Property of Sanilac CMH" on the outside of the carrying case.

Y. Users must not alter the serial numbers and Agency identification numbers of the equipment in any way.

Z. Users must maintain the confidentiality of individuals we serve when using devices. Screens must be protected from viewing by unauthorized personnel, and users must properly log out or put on screen lock when away from their devices. While in the office and plugged in, the computer must be left on to attain any necessary updates pushed out by the IT Department. When transporting turn off computers when not in use.

AA. Users must immediately report any lost, damaged, malfunctioning, or stolen equipment to the IT Department. Any breach of security or confidentiality must be reported to the CIO immediately.

BB. Staff having difficulties with devices should first report trouble by calling or emailing the Help Desk. Problems with computers or any IT equipment should always be reported to the IT department.

CC. Updates to all software programs shall be overseen by the IT Department.

DD. All software programs shall be legally owned or licensed by the CMH, except those that are freely distributed by legal copyright holders or open-source software.

VI. ENFORCEMENT

All supervisors are responsible for enforcing this policy. 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

None

VIII. REFERENCES

IT Security Policy	BA013
Communications Policy	BA070