ST. CLAIR COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE PROCEDURE

Date Issued 03/24

CHAPTER Information Management	**CHAPTER** 08	**SECTION** 001	**SUBJECT** 0010
SECTION Information Systems	**SUBJECT** Computer Information Systems Security		
WRITTEN BY IT Department	**REVIEWED BY** Tommy Rankin	**AUTHORIZED BY** Tracey Pingitore	

I. APPLICATION:

☐ SCCCMHA Board
☐ SCCCMHA Providers & Subcontractors
☒ Direct-Operated Programs
☐ Community Agency Contractors
☐ Residential Programs
☐ Specialized Foster Care

II. PURPOSE STATEMENT:

St. Clair County Community Mental Health Authority (SCCCMHA) shall ensure the proper use and integrity of the agency's computer resources and information systems as delineated herein. Computers, telecommunications, mobile devices, network resources/equipment, software, and the data therein, including the electronic mail system, are the property of SCCCMHA. All employees of the agency must sign a Computer Information Systems Consent statement annually, which acknowledges their agreement to the following administrative procedure.

III. DEFINITIONS:

A. Acceptable Use: The utilization of computing resources in a manner which is consistent with the objectives of SCCCMHA. Use should also be consistent with the specific objectives of the project or task for which such use was authorized. All use inconsistent with these objectives is considered to be inappropriate use and may jeopardize further access to services and/or resources.

B. Agency Electronic Resources: Electronic Health Record Systems (i.e., OASIS, SIS, CAFAS) or electronic files such as E-mail, Files or Folders stored on SCCCMHA owned computer equipment.

C. Attachments: Files that are attached to and sent with e-mail messages.

D. Download: To transfer a file or program from remote servers to your own local system or removable storage device; to save a page or file from the Internet.

E. Electronic Mail (E-mail): Electronic messages that are transmitted between e-mail clients over communications networks.

F. Harassment: Includes, but is not limited to, offensive, maliciousness, profanity, sexually explicit content, race, natural origin or gender specific comments or threats.

G. IT Hardware: Includes personal computers (PCs), mobile devices, servers, routers, switches, printers, monitors, speakers, modem, digital camera, scanner, IP phone, removable storage devices, etc.

H. IT Staff: Refers to those individuals who are employed by the agency who work directly with computer and telecommunications resources in the IT Department.

I. Personal Use: Refers to any use of computing resources which is not related to the business activities of SCCCMHA.

J. Software: The programs (sets of instructions) that tell the computer what to do. There are two types: operating systems software (i.e., Windows) and application software (i.e., MS Office products, OASIS, etc.)

K. User: Refers to all employees, independent contractors, contract agencies and other persons or entities authorized to access or use the agency computer network and telecommunication resources and services.

L. Virus/Malware: A computer code or program that is designed by a person, or persons, to cause harm to a computer. The downloading of files or software from the Internet, or the copying of files from an infected computer workstation to the agency network or workstation can infect a computer.

IV. STANDARDS:

A. Agency Owned IT Hardware & Software

All computer equipment owned by SCCCMHA is the property of SCCCMHA. All electronic data within this system is the property of SCCCMHA.

Users shall not intentionally damage, disassemble (including the removal of asset tags or equipment serial number tags), fix, move, or alter computer software or hardware components. Users may not install software to workstations or the network. Impromptu audits will be performed electronically in order to ensure compliance. IT staff may be required to perform duties, for IT security audits or troubleshooting purposes, which contradict these rules. These may include, but not limited to: altering passwords, logging in as a general user, downloading files, reconfiguring hardware and software.

No individual may remove software or hardware from an agency owned workstation, mobile device, or server for personal use, or bring in software or hardware to use on agency owned equipment. Any duplication of licensed software, except for backup purposes, may be in violation of the Federal Copyright Act. Individuals must adhere to all software license agreements. License agreements vary among suppliers and hardware may need specific drivers or software to operate properly, therefore loading of all agency software and drivers must be authorized by the Information Technology (IT) Department to ensure compliance with licensing agreements and that the software and drivers are virus free.

All new IT hardware and software purchases, including requests for upgraded hardware/software, will be purchased, only when, and if, it fits the context of the Agency's IT Annual Plan and/or budget or is authorized by the Chief Executive Officer or a Director. When there is a need for new/updated IT hardware/software, the supervisor should submit a ticket through the Helpdesk system.

B. Agency Network Access & Use

Agency staff is given access to the agency network and resources using a unique user login ID and password. Users are restricted to accessing only those systems authorized for use on the network. Only those users who have proper rights may gain access to authorized folders and applications. Users must not browse, access, copy or change private or network files for which they clearly have no authorization.

Users shall respect the privacy of others. Users will not represent themselves as other users. Users are required to safeguard their passwords for all systems. Passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. Users are required to "log off" or "Lock Computer" whenever they leave their workstation throughout the business day. Failure to do this allows anyone access to view or edit files under the user's credentials. Leaving a computer unattended and unlocked is a violation of the SCCCMHA Protected Health Information – Privacy Measures administrative procedure #08-002-0005 and Health Care Information Privacy & Security Measures (HIPAA) administrative procedure #08-002-0006.

IT Staff will reset a user's password, as necessary, to complete technical support tasks. Users will not be responsible for transactions made during this process. All users will be required to change their password once the technical support task has been completed.

Any need to contact external vendors to add, modify, and delete software or passwords must be coordinated through the IT Department and must be approved by the Chief Executive Officer or Designee. The IT Department will notify programs/agencies when a SCCCMHA contracted vendor will be visiting their site to work on any agency-owned IT equipment. Vendors/contracted staff shall complete and submit the Computer Acceptable Use Agreement (Form #205) prior to providing services

The IT Department reserves the right to remove shared file/folder permissions, when appropriate and with Leadership directive, as staff members terminate employment or are re-located within the organization and shared file needs are re-evaluated based on job functionality.

Supervisors should submit the appropriate Access Request ticket through the Helpdesk system, as outlined in the Procedures section of this administrative procedure, to request/disable staff user accounts, respectively. Once these Helpdesk tickets have been received, the IT Department will disable the login for the network and follow the instructions of the Supervisor to handle e-mail, voicemail and file folder contents. Supervisors may also request access to their staff electronic resources to ensure program coverage needs are met.

Accessing agency electronic resources on equipment not owned by SCCCMHA is strictly prohibited unless approved by the Chief Executive Officer or Designee in writing. The written document must state the designated user has permission to access specific agency resources on equipment not owned by SCCCMHA and must be signed by the Chief Executive Officer or Designee. This signed document will be attached to the Computer\Information Technology Consent (Form #201) and placed in staff's personnel file and must be renewed annually.

Staff, with Chief Executive Officer or Designee approval to access agency electronic resources on non-agency equipment, must abide by the Personnel: Work Schedules; Leavetime; Overtime; Timecards administrative procedure #06-001-0075, in regards to work hours recorded on their time sheet.

C. E-Mail Usage

The electronic mail system is to assist SCCCMHA in conducting day-to-day business activities. Users are encouraged to consider written documents for formal communication and face-to-face conversations for informal communication as an alternative to using the e-mail system. Only authorized personnel are to use/access e-mail.

E-mail messages, either composed or received in this system, are considered SCCCMHA records and may therefore be subject to Freedom of Information Act requests and other legal disclosure.

SCCCMHA reserves the right to monitor all e-mail messages, either composed or received, in the e-mail system. The employee has no privacy rights at all when sending or receiving e-mail messages.

The confidentiality and privilege sections of the Michigan Mental Health Code and the Privacy Regulations related to HIPAA regarding consumer information apply to the transmission of information in internal and external e-mail resources. Information needs to be de-identified or made reasonably secure and encrypted, when applicable. Identifying consumer information should not be used on e-mail sent to someone outside the agency. Users should exhibit care in drafting e-mail and other electronic documents. Others may review anything created on the computer.

All e-mail is the property of SCCCMHA. The agency reserves the right to override any individual password and access all e-mail messages in order to ensure compliance with this administrative procedure and in the case where an employee is unavailable.

E-mail messages deleted by the user may be retrievable from the e-mail server, e-mail archive server, backup replications or the receiving or sending e-mail filtering systems.

D. Internet Usage

The Internet offers global access to information. Not all sources on the Internet provide information that is accurate, complete or legal. SCCCMHA is unable to monitor or control the content of Internet information, which changes rapidly and unpredictably. SCCCMHA Internet users will need to evaluate for themselves the validity of information found. The availability of information via the SCCCMHA's service does not constitute an endorsement of that information by SCCCMHA. The Internet, as accessed by signing on through SCCCMHA’s workstations, may contain information that is controversial, explicit or offensive. While the IT Department has blocked some sites due to legal liability, security risks, or sites deemed as unnecessary for business use, employees should use the Internet at their own risk.

The Internet is not a private medium to transmit information. Data can be traced, tracked and stored at various components from the origination to the destination of the transmittal. Employees should not expect privacy in any transmission they create, send or receive on computer resources. SCCCMHA reserves the right to monitor all internet traffic coming through the network.

Correspondence transmitted on the Internet is considered legal transmission of documents. E-mails, for example, can be entered as evidence in a court of law. Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or other unlawful material may not be sent by e-mail or other form of electronic communication or displayed or stored on agency computers. Users must respect the legal protection provided by copyrights and licenses to programs, data and images. Computer resources are not to be used in ways that violate legal, ethical or professional standards.

E. Phone Usage

SCCCMHA provides staff the ability to send and receive phone calls to internal staff and individuals outside of the agency. Supervisors may request telephone usage records for their employees by contacting the IT Director or IT Supervisor. Records may also include SCCCMHA provided mobile devices.

F. Agency Network Security

The IT Department will take necessary measures to protect against threats to the agency network and resources. Protective measures such as a firewall, 128-bit encryption of data, user authentication and local machine policies will be utilized to protect against intruders or unauthorized access to systems. The IT Department will also keep agency PC software updated with the latest security patches required. In the interest of energy conservation, staff should shut down their PC and turn off their monitor on a nightly basis unless otherwise stated by the IT

Department. Nightly backups ensure data can be restored in the event of disaster. All users are strongly encouraged to save files in their designated folders on file servers for this purpose. Users should not save any files or data to their local workstation or desktop. This information is not backed up and is not “protected or secure”.

To protect the computer/information system from PC viruses and the potential dangers that viruses create; downloading software, the use of CD-ROMs, DVDs or removable storage from home, vendor, or any outside source for use at the agency is prohibited. Users must be authorized by SCCCMHA Leadership to use removable storage devices (including USB thumb drives and external drives) or CD-ROM/DVD-ROM drive in any equipment on the SCCCMHA network. Attachments to e-mail, file downloads, or data accessed from removable/storage media will automatically be scanned for viruses in an effort to keep the SCCCMHA network free from any damage.

Storage of information on Leadership approved removable/storage media, other than IT Department annual backups, is to be utilized only temporarily, as a last resort, and in emergent situations. This includes, but is not limited to, data copied from, OASIS, Data Management Reports, Financial Information and Contract Management. Data that is temporarily copied to hard drives (such as laptops for business) or removable storage devices, need to be encrypted by means of a secure thumb drive issued by the SCCCMHA IT Department or by software encryption, password protected and ultimately deleted from the temporary device location.

G. Unauthorized/Improper Use Of Agency IT Resources

SCCCMHA reserves the right to monitor any and all aspects of computer use and telecommunications to ensure compliance with this administrative procedure. Computer and telecommunications resources belong to the agency and may be used in a manner consistent with the public service, research and administrative objectives of the agency. Personal use of these resources must be limited to authorized break periods and minimal incidental use. As an illustrative example, printing personal documents must be limited to no more than 10 pages per month.

Abuse or improper use of equipment is strictly prohibited and subject to disciplinary action in accordance with the Personnel: Corrective/Disciplinary Action administrative procedure #06-001-0055. The following list includes, but is not limited to, the type of activity which would be defined as unauthorized/improper use:

1. Engaging in any e-mail activity that would create liability for SCCCMHA.

2. Creating offensive or malicious messages, including, but not limited to, messages that contain profanity, sexually explicit content, race, natural origin or gender specific comments, threats or harassment. Users must comply with all board policies regarding sexual, racial and other forms of harassment or discrimination. Please refer to SCCCMHA Personnel: Harassment in Workplace board policy #06-001-0105 for details regarding this issue.

3. Misrepresenting one’s identity to compose or intercept messages.

4. Revealing your PC username and/or password to another employee.

5. Using e-mail for the purpose of lobbying, religious or political purposes.

6. Using the e-mail system for illegal gambling, betting pools, or investment clubs.

7. Chain letters.

8. Inappropriate use of protected health information.

9. Using agency equipment to perform work for another employer (not SCCCMHA).

10. Any use of e-mail, which violates state and/or federal law, is prohibited.

11. Copyright infringement.

12. Forgery.

13. Plagiarism.

14. Software piracy.

15. Vandalism.

16. Mental Health Code and/or HIPAA violations.

Cessation of service, whether by network disconnection or disablement of staff login ID, may be utilized when remedying or investigating instances of alleged disruption, unauthorized, or improper use of the agency's system.

V. PROCEDURES:

A. Agency Owned IT Hardware & Software

Supervisors

1. Submits a ticket via the Helpdesk system completing the required fields.

IT Director or IT Supervisor

2. Assigns Helpdesk ticket/s to IT Staff.

IT Staff

3. Completes Helpdesk ticket assigned by IT Director or IT Supervisor.

B. Agency Network Access & Use

Supervisor

1. Submits the New User Access Request ticket for new employees, found on the Helpdesk system, to the IT Department at least 24 hours in advance of new hire start date.

2. Submits the Remove User Access Request ticket for terminated/retired/separated employees, found on the Helpdesk system, to the IT Department as soon as last day of work for employee is known. Termination requests needing immediate attention should also be followed up with an e-mail or a phone call to the IT Director or IT Supervisor.

3. Submits the Modify User Access Request ticket for Leave of Absence (LOA) employees, found on the Helpdesk system, to the IT Department as soon as last day of work for employee is known.

4. Contacts the IT Director or IT Supervisor to request usage reports for auditing and compliance.

IT Director or IT Supervisor

5. Assigns Access Request Helpdesk ticket/s to IT Staff.

IT Staff

6. Completes actions requested by Supervisor according to the Helpdesk ticket.

C. Agency Network Security

IT Director or Designee

1. Ensures all agency PCs are kept up-to-date with the latest security patches and anti-virus protection.

Staff

2. Shuts down PC and turn off monitor on a nightly basis unless otherwise notified by IT Staff.

D. Unauthorized/Unacceptable Use of Agency IT Resources

Staff

1. Reports any misuse or abuse of the agency's computer resources and information systems to the immediate supervisor or the next ranking supervisor.

Supervisors

2. Notifies IT Director or IT Supervisor of any staff use of IT resources which violate this administrative procedure. Initiates appropriate disciplinary action in accordance with the Personnel: Corrective/Disciplinary Action administrative procedure #06-001-0055.

IT Director or Designee

3. Monitors agency network for improper use, access, and threats. Compiles reports for management including Internet usage, phone usage, security threats, interruption to network resources, etc. as outlined in the IT Disaster Recovery Plan.

IT Director

4. Determines action to be taken by the IT Department for any violation of this administrative procedure in conjunction with the Chief Executive Officer or Designee.

E. <u>Annual Computer Information Systems Consent – Employee Review</u>

HR Clerical Staff

1. Distributes electronic version of the Computer Information Systems Security administrative procedures with the Computer\Information Technology Consent (Form #201) to all Supervisors and Leadership on an annual basis.

Supervisors/Leadership

2. Forwards the administrative procedures to all of their direct report staff and require they read the administrative procedures and sign the Computer\Information Technology Consent (Form #201).

3. Reads the administrative procedures, sign the Computer\Information Technology Consent (Form #201) and return it to the Human Resources (HR) Clerical Staff.

Staff

4. Reads the Computer Information Systems administrative procedures and sign the Computer\Information Technology Consent (Form #201).

5. Returns the signed Computer\Information Technology Consent (Form #201) to Supervisor.

Supervisor

6. Obtains a signed Computer\Information Technology Consent (Form #201) for each direct report staff.

7. Returns the signed Computer\Information Technology Consent (Form #201) to the HR Clerical Staff.

HR Clerical Staff

8. Obtains signed Computer\Information Technology Consent (Form #201) for all staff.

9. Follows up with Supervisors and Leadership Team on any missing Computer\Information Technology Consent (Form #201).

10. Places a copy of each staffs' Computer\Information Technology Consent (Form #201) in their personnel record (discard previous version of the Computer\Information Technology Consent (Form #201) from the prior year).

VI. REFERENCES:

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

B. HITECH Act of American Recovery and Reinvestment Act (ARRA) of 2009

C. Mental Health Code

VII. EXHIBITS:

A. #0201 Computer/Information Systems Consent

B. #0205 Computer Acceptable Use Agreement

VIII. FORMS:

None Available

IX. REVISION HISTORY:

Dates issued 12/00, 12/02, 12/03, 11/04, 3/06, 06/08, 06/11, 03/13, 09/13, 11/14, 09/15, 8/16, 09/16, 03/17, 03/18, 03/19, 03/20, 03/21, 03/22, 03/23.