St. Clair County Community Mental Health
Providing Opportunities for Health, Wellness, & Connection

Administrative Policy

Policy Title: **Mobile Devices**

Policy #: **08-001-0020**

Effective Date:	06/5/2025
Approved by:	Telly Delor, Chief Operating Officer
Functional Area:	Information Technology
Responsible Leader:	Dann Hayes, IT & Security Director
Policy Owner:	Chase Sherman, IT Technician
Applies to:	SCCCMH Staff

Purpose: To establish detailed standards for the secure and responsible use of SCCCMH-issued mobile devices, with guidance for loss prevention, HIPAA compliance, care, and reporting procedures.

I. Policy Statement

Mobile devices support mobility and service access but introduce elevated risks for data breaches, privacy violations, and equipment loss. SCCCMH-issued mobile devices must be used exclusively for agency business, safeguarded from damage or theft, and returned upon request or termination of employment. Use of mobile devices is subject to agency oversight, and all employees must review, sign, and reaffirm a Mobile Device Agreement annually.

II. Standards

A. Mobile Device Assignment & Agreement

1. Devices are issued with approval from the Chief Executive Officer or appropriate Director.
2. Employees must review and sign Form #0206 Mobile Device Letter of Agreement prior to issuance.
3. The form outlines:
   - Terms of use
   - Financial responsibility for negligent loss or damage
   - Consent to *remote wipe* in case of loss or theft

4. Agreement is saved in the employee's personnel file and renewed annually by employee.

B. Use Expectations

1. Devices are for SCCCMH business use only. Personal use, including by friends, family, or individuals served, is prohibited.
2. Collaborative documentation (e.g., IPOS, releases, periodic reviews) is permitted using agency systems such as OASIS.
3. Employees must bring their SCCCMH-issued devices to work daily. Failure to do so:
   - May require use of a desktop (if available)
   - Will require the employee to use uncompensated time if they must leave to retrieve the device.

C. Device Security

1. Users must:
   - Set a secure password (see Administrative Policy #08-001-0010, Computer Information System Security for standards)
   - Enable automatic screen lock (5-minute timeout or less)
   - Encrypt PHI and use only agency-approved applications
2. Remote access and storage must follow HIPAA and SCCCMH confidentiality requirements.
3. Voice use of mobile phones while driving is allowed only via Bluetooth or when vehicle is not moving and off public roads.

D. Care and Physical Security

To reduce the risk of damage or malfunction:

- Do not install unapproved apps or alter system settings
- Use only SCCCMH-provided power cables
- Do not insert unauthorized USBs or media
- Never leave devices unattended in unsecured areas or vehicles
- Avoid prolonged exposure in hot/cold vehicles or direct sunlight
- Use protective carrying cases when transporting devices

E. Loss, Theft, or Damage

1. Employees must immediately report incidents to the IT Director or Designee:
   - Include:

- Item lost/stolen/damaged
- Last known location and time

2. Reports must be submitted by phone (business hours or after-hours per ADP directory),
3. The IT Department will:
   - Suspend service
   - Activate *lost mode* or remote wipe data
   - Notify the Security and Privacy Officers for HIPAA follow-up
4. Stolen devices require a police report.
5. Financial recovery according to state law and corrective action may apply per agency policies.

F. Return and Recovery

1. Upon separation, leave of absence, or device reassignment, equipment must be returned in working order.
2. HR and the Supervisor coordinate retrieval:
   - HR sends notification to employee with list of items that must be returned
   - Form #0705 Property Receipt Record is completed
3. Equipment is tested, wiped, and returned to IT inventory
4. If necessary, an agreement for employee to pay for lost or damaged equipment and devices is arranged.

III. Procedures, Definitions, and Other Resources

A. Procedures

Actions - Device Assignment

Action Number	Responsible Stakeholder	Details
1.0	Supervisor	1. Identify business need and submit Helpdesk ticket.
2.0	Director/CEO	2. Approve and notify IT
3.0	IT Technician	3. Configure device, review, and collect form #0206 Mobile Device Letter of Agreement.
4.0	Human Resource designee	4. Save signed agreement in personnel file.

Actions - Loss/Damage Reporting

Action Number	Responsible Stakeholder	Details
1.0	Employee	1. Contact IT immediately.
2.0	IT Technician	2. Disable device, track's location, or wipes data.
3.0	Supervisor	3. Submit a Helpdesk ticket to retrieve replacement, when necessary.
4.0	Finance/Payroll	4. Initiate cost recovery for damage/loss, when necessary.

Actions - Return Upon Separation

Action Number	Responsible Stakeholder	Details
1.0	Supervisor or HR	1. Initiate Helpdesk ticket for device retrieval.
2.0	HR	2. Provide signed forms and receipt checklist.
3.0	IT Technician	3. Test, document condition, and wipe device.
4.0	IT Director/ designee	4. Report any unresolved issues to HR/Payroll for potential discipline or repayment.

B. Related Policies

Administrative Policy #06-001-0055, Personnel: Corrective/Disciplinary Action

Administrative Policy #06-001-0075, Personnel: Work Schedules; Leavetime; Overtime; Timecards

Administrative Policy #08-001-0010, Computer/Information Systems Security

Administrative Policy #08-002-0005, Access, Use, and Disclosure of Confidential and PHI

Administrative Policy #08-002-0006, HIPAA Privacy Breach Notification

C. Definitions

1. *Lost Mode:* Device status that disables functionality until retrieved.
2. *Mobile Device:* SCCCMH-owned portable computing device (e.g., smartphone, tablet, laptop.
3. *Remote Wipe:* Deletion of data to prevent unauthorized access in the event of theft/loss.

D. Forms

#0206 Mobile Device Letter of Agreement

#0705 Property Receipt Record

E. Other Resources (i.e., training, secondary contact information, exhibits, etc.)

N/A

F. References

N/A

IV. History

- Initial Approval Date: 05/1990, complete revision 04/2025
- Last Revision Date: 03/2023 BY: Tommy Rankin
- Last Reviewed Date: 04/2025 BY: Dann Hayes and Chase Sherman
- Non-Substantive Revisions: N/A
- Key Words: cell, phone, mobile, laptop, lost, damage, property, financial, access, agreement, leave of absence, termination, retire