**10.00 System Management** *Effective Date: 4/01/2023*

**10.03 System Security and MI-WIC Access**

**PURPOSE**: To provide process requirements local agencies must follow to protect client confidentiality, authorize access to the MI-WIC System, and prevent theft of system-related equipment.

**DEFINITIONS:**

***Privileged user*** means a user that is authorized to perform security-relevant functions that ordinary users are not authorized to perform, such as approval of access requests to MI-WIC and role assignment.

**A. POLICY**

1. System-related equipment and telecommunication resources that are purchased with WIC funds must be used for business purposes only.

2. Local agencies are responsible for maintaining security measures to safeguard all WIC system-related equipment.

3. Physical Security
    a. Stationary computers will be equipped, when reasonable, with devices that secure hardware and deter theft.

    b. Portable equipment will be under the supervision of clinic staff and will be stored securely.

    c. Local agencies will maintain current anti-virus software on all WIC computers use for MI-WIC.

    d. Local agencies will maintain a supported operating system on all WIC computers used for MI-WIC. (See Exhibit 10.02A MI-WIC Workstation Configuration Procedures.)

    e. All computer workstations must be positioned or located in a manner that will protect and minimize the exposure of any client data from unauthorized persons.

    f. Local agency staff must comply with state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

4. User Requirements for System Security

    a. Only local agency staff that directly provides WIC services or supervise staff that provides WIC services will be granted access to the MI-WIC system.

    b. State workers must register at the MILogin website at https://miloginworker.michigan.gov and Third Party / Local Agency users must register at https://milogintp.michigan.gov to obtain their own distinct account prior to subscribing to MI-WIC. (See Exhibit 10.03A Creating a State of Michigan MILogin Account for State and Third-Party Users and Subscribing to MI-WIC.)

    c. User IDs and passwords to access computer devices, MILogin, and software applications must be stored in a secure manner and will not be shared with other individuals.

    d. Each MI-WIC data system user will read and electronically acknowledge the MI-WIC User Security and Confidentiality Agreement prior to accessing the MI-WIC application after they have applied for a MILogin account. The MI-WIC User Security and Confidentiality Agreement is displayed as a pop-up when a user first attempts to access the application and every time this document is updated.

        i. All MI-WIC users will be required to read and electronically acknowledge the MI-WIC User Security and Confidentiality Agreement on an annual basis and when the MI-WIC Security and Confidentiality Agreement has been modified.

        ii. The MI-WIC Security and Confidentiality Agreement acknowledgements are maintained in MI-WIC for as long as the agency staff member has access to MI-WIC confidential information.

        iii. The staff must also sign, and the agency retain, exhibit 9.02A Employee Confidentiality and Compliance Agreement Signature Form. (See Policy 9.02 Employee Compliance.)

        iv. When an employee works at more than one WIC agency or is under the direction of more than one supervisor, the employee must create separate User IDs: one for each agency.

5. WIC Coordinator Roles and Responsibilities for System Security

    a. The WIC Coordinator is responsible for the maintenance of all clinic users' access to the MI-WIC system within their local agency. This includes approving and denying new subscribers, adding, or removing roles for current WIC employees, and removing system access from employees whose employment has ended or they are on extended leave.

b. If a WIC Coordinator finds a user ID in MI-WIC Staff Information that does not belong in their agency, they must contact the State agency to have the user removed.

c. The WIC Coordinator shall assign appropriate clinic and roles based on the user's location of work, responsibilities within the clinic, and staff qualifications. (See Policy 1.07, Local Agency Staffing and Training.)

d. To maintain separation of duties at the clinic level, the WIC Coordinator must ensure that a single staff member is not assigned full access to the system unless the clinic is designated as a Temporary or Permanent Single Staff Clinic. (See Policy 9.03, Employee Conflict of Interest and Separation of Duties.)

e. At the time a WIC staff member permanently leaves employment with their agency, the WIC Coordinator must complete the following actions in MI-WIC within 24 hours:

- Ad a termination date for all roles on the LA Roles screen
- Request removal of all State level roles on the State Level Roles screen
- Remove clinics assigned to the staff member on the User Agencies screen and,
- Add a termination date on the User Access Request screen.

f. If a WIC staff member will be on extended leave for greater than 3 weeks, the WIC Coordinator shall insert the staff member's first date of leave into the termination date field of the User Access Request screen but will not terminate roles or remove clinics. This removes their access to the MI-WIC system but preserves their clinic and role assignments until reactivated.

g. The WIC Coordinator must review all their staff roles annually in MI-WIC to verify that the roles assigned to their staff are appropriate and necessary for the completion of their assigned duties.

h. The WIC Coordinator must review staff roles of privileged users, semi-annually.

i. In the absence of the WIC Coordinator, and a designated staff responsible for role changes, a Local agency staff member can request a role change by calling the State WIC office or emailing the MI-WIC System Administrator directly. The MI-WIC System Administrator shall make the changes in MI-WIC and the request will be documented through email.

References:

45 CFR 164.310

State of Michigan Computer Crime Law (Public Acts 1979-No.53)

Cross-references:

1.03 Confidentiality
1.07 Local Agency Staffing and Training
9.02 Employee Compliance
9.02A Employee Confidentiality and Compliance Agreement Signature Form
9.03 Employee Conflict of Interest and Separation of Duties
10.02A MI-WIC Workstation Configuration Procedures

Exhibits:

10.03A Creating a State of Michigan MILogin Account for State and Third Party Users, and Subscribing to MI-WIC