

### **10.0 Equipment Management**

#### **10.01 Equipment Inventory**

*Effective Date:*

**PURPOSE:** To meet inventory control requirements for nonexpendable property (equipment) purchased with WIC funds.

#### **A. POLICY**

1. In accordance with USDA Regulations, each local agency is required to keep an inventory of equipment-related items purchased using WIC Program funds. The inventory records shall include items costing more than \$2500. Items costing less than \$2500, such as computer equipment, printers, scanners, signature pads and multiple-user electric breastpumps (See Policy 11.06 Breastfeeding Equipment, Inventory and Maintenance) must be listed to monitor inventory. A sample inventory form is illustrated in Policy 10.01 Exhibit A. Inventory should include the following:
  - a. Item description, including brand/model
  - b. Cost (if applicable)
  - c. Location assigned, or date salvaged
  - d. Serial Number
  - e. Tag number (optional)
  - f. Date purchased or acquired
  - g. Purchased by (local or State)
  - h. Specific warranty information (if applicable)
2. The inventory shall be updated at least annually and made available for review at Management Evaluation, Accreditation or Audit.
3. Property removed from the inventory listing due to loss or obsolescence must be designated as lost or obsolete and disposed of in a manner that identifies any benefit gained through the disposal as being credited to the WIC Program.
  - a. Deleted property list must be forwarded to the State WIC Program.
  - b. Computers must be stripped of all client information prior to disposal.
  - c. Details regarding any loss must be attached to the inventory.
  - d. If theft was the cause of loss, the agency must follow Policies 9.01 Participant Compliance or 9.02 Employee Compliance, if clients or staff were involved.
4. Inventory records must be retained for 3 years and 150 days after the end of the fiscal period, or until any outstanding audits are completed. Records for items removed from inventory shall be retained for 3 years after final disposition (sale, donation or landfill).
5. Capital expenditures over \$2500, such as the cost of facilities, equipment, including medical equipment, other capital assets and any repairs that materially increase the value of useful life of capital assets must be prior approved for purchase by USDA/FNS and MDCH-WIC.

References:

- CFR 246.13 (j) Financial Management Systems
- CFR 246.14 (d) (2) Specified allowable nutrition services and administration costs
- CFR 246.24 (d) Procurement and property management
- CFR 246.25 (a) Recordkeeping requirements

Cross-References:

- 9.01 Participant Compliance
- 9.02 Employee Compliance
- 4.04 Breastfeeding Equipment, Inventory and Maintenance

Exhibits:

- 10.01A Sample Inventory



# **MI-WIC POLICY**

## ***Equipment Management***

### **10.0 Equipment Management**

#### **10.02 Equipment Maintenance and Replacement**

*Effective Date:*

**PURPOSE:** To state local agency responsibilities for maintaining equipment and working with the State for replacement of equipment.

#### **A. POLICY**

1. All computer equipment purchased by MDCH/WIC for the local agency will be covered under a manufacturer's limited warranty.
  - a. It is the responsibility of the local agency to contact the manufacturer for any repair of equipment while under the manufacturer's warranty.
  - b. Once the manufacturer's warranty has expired, it is the responsibility of the local agency to maintain and service equipment, either through a maintenance contract with a local vendor for service/repair or some other arrangement.
2. When WIC-funded computer equipment is no longer used for its original purpose, the equipment may be used in other activities currently supported by the federal agency or related programs (i.e. WIC administrative tasks, other programs within the agency) or salvaged.
  - a. WIC-funded computer equipment that has a current unit value of less than \$5,000 may be retained, sold or otherwise disposed of. Property records must be maintained that include:
    - i. A description of the item
    - ii. Serial number
    - iii. Method of disposal (i.e., donated to charity, used for parts, thrown in dumpster, etc.)
    - iv. Date of disposal
  - b. Document disposition or disposal (salvage) of equipment and send a copy of the document to the WIC Local Agency Liaison. Documentation shall include:
    - i. A description of the item
    - ii. Serial number
    - iii. Method of disposal (i.e., donated to charity, used for parts, thrown in dumpster, etc.)
    - iv. Date of disposal
    - v. Proceeds from any sale (if applicable)
  - c. Computers must be stripped of all client data prior to disposal or use in other programs (See Policy 10.01 Equipment Inventory).

- d. Equipment that is no longer used for its original purpose is not eligible for replacement.
3. If WIC computer equipment is no longer usable due to obsolescence or irreparable damage, the local agency can request replacement of the equipment. WIC Coordinators shall submit computer equipment replacement requests to the State or Local Agency Liaison.

References:

7CFR, Section 3016.32

Cross-references:

10.01 Equipment Inventory

# **MI-WIC POLICY**

## ***Equipment Management***

### **10.0 Equipment Management**

#### **10.03 System Security**

*Effective Date:*

**PURPOSE:** To detail processes local agencies must follow to protect client confidentiality and to prevent unauthorized access to WIC data.

#### **A. POLICY**

1. Computers and telecommunication resources (the Internet) purchased with WIC funds may be used for business purposes only.
2. Local agencies shall maintain security measures to safeguard all WIC equipment.
3. Physical Security
  - a. Stationary computers shall be equipped, when reasonable, with devices that secure hardware.
  - b. Portable equipment shall be under the supervision of staff and shall not be left unattended.
  - c. If portable equipment is used by multiple staff, the local agency shall maintain a log of users and dates equipment is taken and returned.
  - d. Local agencies shall maintain current anti-virus software on all WIC computers used for MI-WIC.
  - e. All computer workstations must be positioned or located in a manner that will minimize the exposure of any displayed client data.
  - 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. System Access
  - a. Each user will have his/her own distinctive Single Sign On account.
  - b. The WIC Coordinator shall be responsible for maintenance of all clinic user access to the MI-WIC system within the local agency.
  - c. The WIC Coordinator shall assign role permissions to users based on their responsibilities in the clinic, and WIC policy requirements.
  - d. At the time of termination from a local WIC agency clinic, or a reassignment to another non-WIC program, all user roles must be removed from MI-WIC for that employee.
5. Local Agency User Requirements
  - a. All local agency staff shall have access to the Internet and MI-WIC.

- b. All users must sign and abide by the terms of a MI-WIC User Security and Confidentiality Agreement (See 10.04A MI-WIC User Security and Confidentiality Agreement).
  - c. User ID's and passwords shall not be shared with other individuals.
  - d. User ID's and passwords must not be documented, written or otherwise stored in an unsecured manner.
6. MI-WIC User Security and Confidentiality Agreements shall be kept current as long as the agency staff member has access to MI-WIC confidential information. The Agreement shall be updated if the employee's role changes within the WIC program. The Agreements shall be retained by the local agency for three years 150 days beyond employment by the local agency.

References:

- 45 CFR 164.310
- State of Michigan Computer Crime Law (Public Acts 1979-No.53)

Cross-references:

- 1.03 Confidentiality
- 10.04 MI-WIC Access

# **MI-WIC POLICY**

## ***Equipment Management***

### **10.0 Equipment Management**

#### **10.04 MI-WIC Access**

*Effective Date:*

**PURPOSE:** To allow local agency users to access the MI-WIC Data System.

#### **A. POLICY**

1. Each MI-WIC data system user must read and sign the MI-WIC User Security and Confidentiality Agreement prior to requesting access to the MI-WIC application after they have applied for a Single Sign On (SSO) account. See Exhibit 10.04A MI-WIC User Security and Confidentiality Agreement.
2. Each user will have his/her own distinctive Single Sign On account.
3. To use the MI-WIC system, all local agency users must register in Michigan Department of Community Health's SSO website at <https://sso.state.mi.us>. If a user does not already have an SSO account they must register with SSO at the above address.
  - a. The user must have an email address to create an SSO account.
  - b. If the user does not have an agency email address, one can be created at [www.yahoo.com](http://www.yahoo.com) or other free email source, or the user may use the WIC Coordinator's email address.
4. The WIC Coordinator shall be responsible for approving, denying and removing clinic staff not authorized to the MI-WIC system within the local agency. Only staff providing WIC services or direct supervision shall be granted access to the MI-WIC system.
  - a. The WIC Coordinator shall be responsible for assigning the appropriate MI-WIC roles to access the MI-WIC system for each user.
  - b. Denying or removing someone from the MI-WIC application does not remove the SSO User ID and password.
5. At the time of termination from a local WIC agency clinic, or a reassignment to another non-WIC program, all user roles must be removed from MI-WIC for that employee.
6. WIC Coordinators will alert the State when an employee is no longer employed in the local agency so the employee's SSO account can be terminated.
7. MI-WIC User Security and Confidentiality Agreements shall be kept current as long as the agency staff member has access to MI-WIC confidential information. The Agreement shall be updated if the employee's role changes within the WIC program. The Agreements shall be retained by the local agency for three years 150 days beyond employment by the local agency.

### **B. GUIDANCE**

1. The SSO account registration process requires the user to provide Challenge/Response answers for later use if a password reset becomes necessary. The user should store the Challenge/Response answers in a safe place.
2. The top portion of the MI-WIC User Security and Confidentiality Agreement should be completed by the user with the following information:
  - a. User Name
  - b. Contact Phone Number
  - c. Workplace Address or Location
  - d. Fax Number
  - e. Email Address
  - f. User Signature and Date
3. The WIC Coordinator or designee will check the appropriate role permissions assigned to the user and sign and date the form.

Reference:

45 CFR 164.310  
State of Michigan Computer Crime Law (Public Acts 1979-No.53)

Cross-Reference:

10.03 System Security

Exhibits:

10.04A MI-WIC User Security and Confidentiality Agreement