Section 9.2: Hardware

07/2026

References: MN Chapter 13 Data Practices Act, 7 CFR 246.26 (d-h); 2027 WIC Grant Agreements, Exhibit A WIC Grantee Duties.

Policy: All Local Agencies are required to provide computers and peripherals, that meet the State's minimum hardware specifications to access the Minnesota WIC Program Information System.

Purpose: To ensure consistency of the system, maximize operation efficiencies, and maintain data integrity and security.

Procedures

Hardware support

Local Agencies must provide their own computers for using the WIC Information system. The State will provide the minimum specifications for the computer hardware needed to efficiently use the WIC Information System. The State will also provide an approved peripherals list that will include scanners, signature pads, and card readers that have been fully tested and approved for use with the WIC Information System.

The Local Agency must also meet the following criteria:

- Provide adequate IT support that is available, responsive, and effective.
- Ensure Local IT support provides and maintains adequate inventory for new staff and replaces faulty hardware within 24 hours.
- Meet State security standards (found in Section 9.4) and minimum hardware specifications.
- Provide specific Windows operating system version and Office Suite.
- Provide real-time anti-virus protection.
- Provide regular security updates to the operating system and anti-virus software and definitions.
- Use full disk encryption software.
- Create a process to ensure temporary files in the Downloads folder MUST be set to delete after 1 day and deleting files from the Recycle Bin MUST be set to no more than 30 days or the state provided Download and Recycle Bin script may be used (See Guidance below).

- Must have a default web browser of either Google Chrome or Microsoft Chromium Edge.

Local Agencies must use the Minnesota WIC Help Desk as the first point of contact when in need of assistance in the event of an issue where the software is causing an issue with the approved list of hardware peripherals.

Physical hardware security

Hardware should not be left in vehicles.

When available, computers should be securely locked to a stationary object using a Kensington Lock or equivalent.

Local Agencies should follow any other local policies regarding physical security of computer equipment purchased using federal funds.

Lost or stolen computer equipment

Due to the risk of a potential data breach (see Section 1.7: Data Privacy), Local Agencies must **immediately** do the following if computer equipment is identified as lost or stolen:

- **Contact Local IT** and follow local protocol for lost/stolen equipment.
- **Contact** the following staff at **State WIC office**:
  - WIC MIS & Data Unit Supervisor
  - WIC Nutrition & Clinic Services Unit Supervisor
  - Agency's State WIC Consultant
- Provide the following information:
  - List of missing equipment
  - Agency name and number
  - Location where loss/theft occurred
  - Date and time the loss/theft occurred (actual if known or estimated)
  - Circumstances around the occurrence
  - Provide a copy of the police report if applicable

Incidents involving lost or stolen equipment that may include unauthorized access to private data must also follow the **cybersecurity incident notification requirements** described in Section 9.4: Network, Browser, and User Access Security.

Training

Annual security training is required for all WIC staff every federal fiscal year. Local Agencies are responsible for ensuring and tracking that all staff view the security module annually each year and new staff view this Security Module as part of Information System training.

- WIC Security Training
- Local Agency Security Training Module Tracking form

Guidance

A Download and Recycle Bin script was created to help Local Agencies meet security requirements after downloading documents that contain private data. This script creates a scheduled task to delete all files from the Downloads folder and the Recycle Bin each time a user logs onto their computer and at 8 pm daily if the computer is not shut down overnight. The Download and Recycle Bin Script and instructions are available from the State office. Local Agencies may use the provided script or create one of their own locally that performs the same function.

Reference – Complete Listing of Hyperlinks

Section 9.4: Network, Browser, and User Access Security
(https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_4.pdf)

Section 1.7: Data Privacy
(https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch1/sctn1_7.pdf)

WIC Security Training
(https://www.health.state.mn.us/people/wic/localagency/infosystem/hubert/training/index.html#security)

Local Agency Security Training Module Tracking Form
(https://www.health.state.mn.us/docs/people/wic/localagency/training/security/tracking.docx)

Minnesota Department of Health - WIC Program 625 Robert St N, PO BOX 64975, ST PAUL MN 55164-0975; 1-800-657-3942, health.wic@state.mn.us, www.health.state.mn.us. To obtain this information in a different format, call: 1-800-657-3942

This institution is an equal opportunity provider.