DEPARTMENT OF HEALTH

Section 9.3 Security of WIC Information System: Networks, Data, and Equipment

06/2017

References: MN Data Practices Act, MN Statute 13.01 – 13.99; Functional Requirements Document (FReD) Version 2017 2.0; MDH Information Security Policy.

Policy: Local Agencies must ensure the security of WIC Information System networks, data and computer equipment. Information obtained from individuals applying for, or participating in the WIC Program is considered private and may not be disclosed to any unauthorized person(s). (See Data Privacy, MOM Section 1.7.)

Purpose: To prevent fraud, avoid theft, and ensure data privacy and integrity.

Procedures:

- Local Agencies must follow local network and Internet usage policies.
- Local Agencies must ensure that all computers use a firewall. This can be a software firewall or a hardware device.
- Local Agencies must contact their network administrators to assist with any planning or installation of any network device or functionality on their network.
- Each staff must use her/his own username and password when accessing the system. The system tracks all activities by username. Never use a computer without entering your unique user name and password.
- It is recommended to create local users' Windows accounts with limited privileges.
- The system will require all users to change their password every 90 days.
- Local Agency coordinators must submit username and password request/change form via the MDH WIC website for both new and departing staff.
- In case of an **unplanned** departure of staff, Local Agency Coordinators must call the Help Desk to **immediately** deactivate the user name account.
- Local Agencies must secure WIC computer equipment and software at all times including during transport and storage; storage facilities must be adequately secured.
- Local Agencies must secure any copies of the Minnesota WIC computer image.
- Local Agencies must maintain the inventory of WIC computer equipment received from the Contractor. The Local Agency must verify its accuracy and work with the Contractor to

make corrections as needed. Refer to Section 9.4, Equipment Inventory – WIC Information System.

- If there is a breach of security, such as stolen computer equipment or media with participant data, Local Agencies must ***immediately*** contact:
  - WIC MIS & Data Unit Supervisor
  - WIC Nutrition & Clinic Services Supervisor
  - State WIC Consultant

  Provide the following information:
  - List of missing equipment
  - Agency name and number
  - Location where loss/theft occurred
  - Date and time loss/theft occurred (actual if known or estimated)
  - Circumstances involved
  - Provide a copy of the police report information if applicable
- All WIC staff must complete required annual WIC Information Security Training. Local Agencies are responsible for Tracking Staff Training and ensuring that all staff review the security module every year.
- Local Agencies should follow any additional or more stringent local security policies.

Guidance

Passwords

Create good (strong) passwords; most importantly, keep your passwords strong:

- Use eight or more characters
- Mix upper-case and lower-case letters with numbers and special characters
- No dictionary words, proper nouns, or foreign words
- Do not use a correctly spelled word in any language, because "dictionary attack" software can crack these in minutes.
- Do not use personal information such as your name (or the name of a relative or pet), birthday or hobby, because these are easy to guess.
- Choose a password that is difficult to guess or hack, but that you can remember without having to write it down. For example:
  - Choose the first letters of words in a title, song or poem. For example, Book One: Harry Potter and the Sorcerer's Stone becomes b1HP&tss

  - String several words together (the resulting password is also known as a "passphrase") and insert numbers and special characters. For example, turn -go to town" into go2^*ToWn
  - Insert punctuation or numbers into a regular word. For example, turn "regular" into rEgu!4lar
  - Deliberately misspell a word (don't use a common misspelling). For example, turn "common" into koM*7on Use
- Changing your password means to “significantly” change your password. Changing just a letter or a number or two in your password is not considered “significantly” changing your password. Your password should also be changed immediately if you think for any reason it could have been compromised.

Protect your Password

Your password is secret and confidential; be sure to keep it that way. Never share your password to anyone, whether in person or over the phone -- no matter who asks, no matter why they say they need it.

Intruders look for passwords posted on your computer, under your keyboard, inside your desk, on your bulletin board and in every other area of your workspace. This is why it is best not to write down your password at all. If you must write down your password, treat it like money and keep it in your wallet or another secure location. If you take a laptop out of the office, please ensure that the password is not written down on the laptop or in the computer bag. Use a completely different password scheme at work and home. If the password you use at home were to be compromised for any reason, we would not want that situation to cause your work computer accounts to be put at additional risk of compromise**.**

Other Security Measures

Enable Screen Savers

Enable screen savers with passwords on all computers/devices. This protects the confidentiality of participant data and protects the logged-in user from other staff entering data, making modifications, or creating benefits cards.

Lock Computers

A workstation should also be locked when not in use or when left unattended. Press Ctrl + Alt + Del sequentially and click the Lock command. (Or, press the Windows key + then ‘L’ to lock the computer.) The logged in user will need to enter their password to unlock the computer.

Kensington Locks

- Use Kensington Locks to secure all desktops and laptops to stationary objects.
- Kensington Locks come with two keys.
  - The spare key should be stored in a secure location.
  - The key used daily should be kept on your person while the lock is being used and not stored in your desk drawer or bag.

Transportation of Equipment

Computers, scanners, signature pads, cards, and card readers should not be left in automobiles overnight. Bring equipment inside to protect them from theft and extreme temperature changes.

Removable Storage

An acceptable use of removable storage is: copying documents and screen shots from a WIC computer for printing on a non-WIC printer.

Other Removable Storage Guidelines:

- Storage of data on removable media or devices is meant for short-term use only and should be removed immediately after its use.
- All removable storage that contains ANY participant information should be protected at the same level as other computer equipment.
- When not in use, store the removable storage media and devices in a locked location, such as a locked desk or locked file cabinet
- All removable storage media and devices should be treated as if they contain private information even after they have been erased.
- WIC-associated paper, CD or DVD material, which contains participant data, should be erased, broken, or shredded before disposal.

Reference – Complete Listing of Hyperlinks

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

Section 9.4, Equipment Inventory – WIC Information System (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_4hubert.pdf)

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

Tracking Staff Training
(https://www.health.state.mn.us/people/wic/localagency/infosystem/training/security.html)

Minnesota Department of Health - WIC Program 85 E 7th Place, PO BOX 64882, ST PAUL MN 55164-0882;
651-201-4444, health.wic@state.mn.us, www.health.state.mn.us;
To obtain this information in a different format, call: 651-201-4444