Section 9.4: WIC Information System – Network, Browser and User Access Security

AUGUST 2023 - DRAFT

References: MN Statutes Ch 13 MN Data Practices Act; 7 CFR 246.26 (d-h), Minnesota WIC Annual Security Training Module

Policy: All Local Agencies must provide a secure environment in which staff can access the WIC Information system and ensure browser and user security requirements are met.

Purpose: To ensure data privacy and the integrity of the Minnesota WIC Information system by ensuring network, browser and user security requirements are met.

Procedures

Network Security

Local Agencies must provide technical support for initial set-up, maintenance and support of a network including any ongoing internet connectivity issues.

Local Agencies must work with their network administrators to assist with any planning or installation of any network device.

Internet support can be from county or Local IT staff, contractor, or Internet Service Providers.

Secure wireless connectivity options can be used when a wired communication cannot be achieved.

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 hardware device.

Browser Security

The **only** approved browsers by which you can access the WIC Information system are:

- Google Chrome
- Microsoft Chromium Edge

If prompted by the browser, **NEVER** select to save your username and/or password to the browser.

The WIC Information System should only ever be open in one browser at a time.

The WIC Information System should only ever be open in one tab of the browser at a time.

Only one of the WIC Information System environments (Production, Training, Office) should be open in a browser at a time.

The downloads folder of the browser **MUST** be set to be cleared or deleted after 1 day and the Recycle Bin MUST be set to delete files permanently at no more than 30 days. This can be done by a manual or automated process. (See Guidance)

User Access Security

When using State-provided hardware, local users' Windows accounts should be created with limited privileges.

Each user with access to the WIC Information System **MUST** have a unique county or agency-maintained email address to allow for use with Multifactor Authentication (MFA) when logging into the WIC Information System.

Each use **MUST** ensure they are receiving the MFA daily.

Each staff member **MUST** use their own username and password when accessing the WIC information system.

Each user should only be logged into one WIC Information System Environment at a time.

Each user should only be logged into one browser window/tab at a time.

Each user should only be logged into one workstation at a time.

Only a Local Agency WIC Coordinator or their designated alternate may submit requests to the state for the following user activities related to the WIC Information System:

- New user access requests
- Deactivations for current users
- Updates to current user's access roles

In the case of an **unplanned** departure of staff, a Local Agency Coordinator or their designated alternate, must call the Help Desk **immediately** to have the username deactivated.

In the case of a planned leave of absence or vacation lasting four weeks or longer, the Local Agency Coordinator or their designated alternate must submit a request to have the staff member's username place on "HOLD". When the staff person returns from the absence, the

Coordinator or designated alternate should submit a user access request to have the staff member's username HOLD status removed.

Password Security

Passwords **MUST** meet the Minnesota Department of Information Technology Services requirements for passwords. Passwords must include the following:

- Eight or more characters in length
- At least 1 (one) upper case letter
- At least 1 (one) lower case letter
- At least 1 (one) number
- At least 1 (one) special character

The WIC Information System will require passwords to be changed every 90 (ninety) days.

The WIC Information System will not allow any of the past 9 (nine) passwords to be reused.

Your password is confidential; be sure to keep it that way. Users should do the following:

- Never share your password with anyone whether in person or over the phone, no matter who asks or why they say they need it.
- Never keep your password written down, either under your keyboard, inside your desk, on your bulletin board or anywhere else in your workspace.
- If you must write down your password it should be kept on your person or in another secure location.

If you believe for any reason that your password has been compromised, change it immediately.

Enable screen savers with passwords on all computers.

When you step away from your computer you must always lock your computer to ensure that any private information on your screen is not seen by someone walking by.

Guidance

Network Security Guidance

Whenever possible when working remotely a Virtual Private Network (VPN) should be used.

If a wireless network is used it is recommended that a security protocol be used. It should either require a user to agree to legal terms, register an account, or type in a password before connecting to the network.

Downloads from a Browser

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 now available and can be downloaded from FileZilla, Agency Gateway/Download and Recycle Bin Script.

Password Guidance

Passwords should follow the following guidance:

- Do not use common words, names, and/or keyboard sequences.
- Do not use the same password for all your sites.
- Do not use a correctly spelled word in any language.
- Do not use personal information such as your name (or that of a pet or relative), birthday, or hobby.
- Do not use references to favorite sports teams, numbers, or movies.
- Choose something that is difficult to guess but something you can remember without writing it down.
- 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
- Choose a passphrase where several words are strung together adding numbers and special characters.
  - For example, go to town becomes go2^ToWn
- Choose to insert punctuation and numbers into regular words.
  - For example, regular becomes rEgu!4r
- When changing your password change it significantly, changing just a letter, a number or two in your password is **not** considered changing it significantly.

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.