

III. Information Systems

3.1.040 WIC Applications Access, User Names, Passwords and Security

Authority 2008 7 CFR 246.26 (d)
Issued 01/1993
Revised 01/2011

POLICY: To maintain proper security and participant confidentiality, each individual who accesses the WIC data system must have his/her own user identification (UserID).

For new employees, the local agency (LA) administrator or the WIC coordinator shall submit an Automated Security Access Processing (ASAP) form to add WIC system access one week prior to the employee's first date of employment or as soon as possible after employment begins.

When individuals no longer need WIC access or if employment is terminated for any reason, the LA administrator or WIC coordinator shall submit an ASAP form to delete WIC access as soon as possible.

The LA shall ensure that WIC staff do not share individual user names and passwords.

The LA staff shall logout of WIC applications when away from their desk or when another person will be working at their computer for any amount of time. For short periods of inactivity, password protected screen savers shall be activated on all workstations.

When the sharing of an individual user name and password is discovered through desk audit, monitoring, or other means, the state WIC technical assistance (TA) team shall follow the sanction guidelines detailed in this policy.

PROCEDURES:

- A. When state and local WIC provider (LA) staff members need to access the WIC data, the Missouri WIC Information Network System (MOWINS), the WIC electronic reports, the web-based Local Agency Plan (LAP), and the web-based WIC Administrative Cost Invoice (WIC-24) or need additional data system access, they must do the following:
 1. Complete the required online request form ([ASAP](#)) stating the access needed.
 - a. Add user name and access for new employees or employees who have not previously used the program application(s) listed above.
 - b. Add additional access if user name already exists.
 - c. Revoke user name when an employee leaves employment.
 - d. Revoke program application access when it is no longer needed.
 - e. Change identifying information such as a name or agency employment change.
 2. Refer to the state WIC web site [Missouri WIC MOWINS Help Desk](#) for [ASAP](#) instructions to access MOWINS.

- B. An e-mail notification will be sent to the individual and the WIC coordinator when access is granted.
- C. Retain copy of all ASAP requests in a central file for monitoring purpose.
- D. User names and passwords are an important aspect of computer security. All state agency (SA) staff, LA staff, contractors, subcontractors, and any other temporary staff person or person(s) with access to MOWINS must have unique user names and personal passwords. All staff and contractors need to comply with the following:
 - 1. Be responsible for all information entered and functions performed for the entire period s/he is logged on.
 - 2. Exercise all security requirements to protect integrity and confidentiality.
 - 3. Not share their user name and password with any individual, including applicants, participants, and other WIC staff.
 - 4. Take all precautions and efforts necessary to protect the visual observation of their user name and password when they enter it into MOWINS.
- E. MOWINS is set up to track user name, date and time the system is accessed. The "View System Access Log" feature in MOWINS will be used by the SA staff to monitor compliance.
- F. Security violation - when the sharing of user name and password is discovered, the state WIC TA team shall follow the sanction guidelines listed below.
 - 1. First offense: The state WIC technical assistance (TA) team will contact the local WIC coordinator or the WIC administrator by phone and relate to him/her the suspected security violation and the opportunity to cease the activity. The state TA team will summarize the conversation in an e-mail for future reference. This is considered a verbal warning.
 - 2. Second offense: If the sharing of user name and password violation continues after the verbal warning, the state WIC TA team will send a letter to the local WIC administrator detailing the second violation. The LA will be notified in the letter that if the violation continues, the SA will impose a fine to the LA. The LA must respond with a corrective action plan within 15 calendar days.
 - 3. Third offense: If the LA staff is found in violation a third time, the LA will be sanctioned and receive a \$100 fine. The LA must pay the state within 30 calendar days using non-WIC funds. Failure to pay the fine may result in the withholding of the monthly WIC administrative cost reimbursement.
 - 4. Fourth offense: If the LA staff is found in violation a fourth time, the SA will revoke the individual's access to MOWINS. The SA will recommend to the LA that the violator be disciplined according to LA policy.