POLICY AND PROCEDURE MANUAL

1. GENERAL ADMINISTRATION

1.08 Information System Management

A. POLICY

The security and accuracy of the highly-sensitive participant information maintained within the WIC Management Information System (MIS) must be ensured to comply with federal and Commonwealth regulations and safeguard the welfare of the program's participants, and correlatively the integrity of the program. Therefore, state and local agency staff must account for the physical location and security of system-connected hardware, including desktop and laptop PCs, at all times. This involves adhering to guidelines for creating and maintaining user IDs and effective passwords and updating the system routinely. Proper procedures for capturing clinic staff and participant signatures must also be followed to adhere to regulations and protect against fraud.

B. PROCEDURE

1. Equipment Management

a. When requesting additional computer equipment or wiring, or moving, closing or opening a clinic, staff must fill out the Data Equipment Request (DER) (Attachments 1 & 2). The DER form shall be submitted to the State Agency seventy-five (75) days prior to the expected date of change or sixty (60) days prior for equipment requests only.
b. No computer equipment shall be moved without State Agency approval. The Transfer Equipment Request (TER) (Attachments 2 & 3) will be filled out and must be approved prior to moving any computer equipment. The TER must be submitted to the State Agency before equipment can be transferred. The Transfer Equipment Request form must be submitted thirty (30) days prior to transfer.
c. When leaving a desktop or laptop computer unattended, users shall apply the "*Lock Workstation*" feature (ctrl/alt/delete, enter).
d. Commonwealth approved encryption software is required on all WIC laptops whether they are purchased by the Commonwealth or with NSA funds by the Local Agency.
e. Desktop and laptop computers shall be set to time-out after fifteen (15) minutes of non-use and staff will have to resign into the WIC MIS system.
f. A physical inventory must be completed annually of all computer equipment (desktop PCs, printers, laptops, etc.) and sent into the State Agency using the Physical Inventory Form (Attachments 5 & 6).
g. Individual users shall not install or download software applications and/or executable files to any WIC desktop or laptop computer without prior authorization. All software shall be loaded via SMS.
h. There shall be no personal use of desktop PCs or laptops.

i. All computer equipment used strictly for administrative purposes must be purchased with NSA funds and each Local Agency will be responsible for keeping the equipment updated with security patches. Equipment purchased by a local agency for administrative use shall never be connected to the state network and shall only be used for WIC purposes.
j. If computer equipment is lost/stolen, report all security incidents to your Local Agency clinic manager immediately, who must report the incident to the state police immediately and notify the State Agency within twenty-four (24) hours.
k. All equipment purchased through the Bureau of Information and Technology (BIT) must be used for the WIC MIS system only.
l. All equipment that is purchased through BIT will be maintained by BIT. Any equipment that is purchased with NSA funds is the responsibility of the each Local Agency to maintain.
m. Equipment purchased through BIT must be returned back to BIT when replacement equipment has been purchased. Equipment that is purchased with NSA funds must be disposed of in accordance with Policy 3.03 Documentation of Expenses.
n. Users should log off at the end of each day, but desktop PCs should be left powered on so that security patches and updates can occur as necessary.
o. All laptops should be kept at the primary clinic site, according to inventory records. Primary clinic is where the laptop is stored and connected to the network. If a laptop is moved to another primary clinic site, a Transfer Equipment Request form is required to be filled out. (Attachment 4)

   1. Local agencies shall use a log (Attachments 7 & 8) to track the location of laptops.
   2. Logs should be kept at the primary clinic site and not with the laptop.
   3. Laptops shall be protected from temperature extremes, precipitation and dampness.
   4. Laptops shall be transported in their protective carrying cases at all times.
   5. Laptops must be locked via CTRL/ALT/DELETE or logged off via the START button when not attended by staff.

2. Connection to Network (commonwealth-purchased equipment only)

a. All laptops must be connected to the Commonwealth network at a minimum of once per week in order to assure synchronization with the WIC MIS system, as well as receipt of vital security patches and updates.
b. Laptops must be connected to the network by 6:45 pm in order to be synchronized on any given evening.

c. Successful synchronization of the laptop must be verified on the login screen. The date of successful synchronization must be noted on the log before the laptop is taken to the satellite clinic.
d. If synchronization is not successful after two consecutive attempts, an incident report must be submitted that includes the affected Computer's Name (DOH Number).
e. All laptops should not be connected at one time to synchronize. Only connect two (2) to three (3) laptops at a time.

3. Laptops that are assigned to a staff member(s) are the responsibility of the staff member(s) until they are returned.
4. Laptops shall not be used when directly connected to the network at a primary site.
5. Digitized Signatures

a. The State Agency has elected to capture secure electronic digitized signatures to meet WIC Program signature requirements in both the administration of the program and for endorser/participant signature capture. This digitized signature policy is compliant with the security requirements outlined by USDA and the Commonwealth of PA. Digitized signatures will be captured and maintained in accordance with record retention requirements.
b. The State Agency has elected to electronically capture digitized signatures as documentation of Food Instrument receipt by Endorsers/Authorized Representatives, Income Verification by Staff and Verification of Certification information on the Participant Data Form (PDF) by Endorsers/Authorized Representatives and Staff. All Endorsers/Authorized Representatives and staff will be notified that their legal liability and level of obligation undertaken when signing for WIC FIs, income verification or on the PDF form is the same whether captured electronically through the digital signature pads or a handwritten signature on the FI receipt, income verification receipt or paper PDF document.
c. The WIC State Agency shall require paper documents in the following circumstances:

1. WIC staff who act as Endorsers/Authorized Representatives
2. WIC staff that reissue FIs to vendors
3. FIs that are being mailed to the Endorser
4. Operational failure of the digitized signature pad

6. Staff shall comply with all policies related to fraud prevention and control and the separation of duties that are contained in this Policy and Procedure Manual.

7. The digitized signature image will be captured and maintained in the FI record. Paper receipts signed by Endorsers/Authorized Representative shall be maintained in chronological order by day of issue or in the participant’s file. Paper receipts for FIs mailed or reissued to a vendor shall include the User ID and name of the staff person who printed the FI and shall be maintained in the participant’s/vendor’s file. Paper receipts for the income verification signed by staff shall be maintained in the participant’s file. Paper PDFs signed by staff and applicant shall be maintained in the participant’s file.
8. One (1) digitized signature pad will be provided for every WIC personal computer, including laptops, at each Local Agency.
9. The digitized signature pads are to be used in accordance with State Policies related to digital documentation of the provision and receipt of WIC services, including certification and benefit issuance.
10. Each local agency clinic manager shall be responsible for assuring staff compliance to all security policies and procedures and all activities related to the digitized signature pad use. All Local Agency program reviews shall include a review of digitized signature compliance.
11. Access to digitized signature records will be provided to staff with security access to the FI lookup and FI archive lookup tabs, certification and income histories within the MIS.
12. Connectivity problems or malfunctions should be reported to the Help Desk immediately.
13. Signature recordkeeping

    a. Records will be displayed in the FI Lookup and FI Archive Lookup areas, certification history and income history. If the digitized signature pads are not working follow the procedures listed below.
    b. Paper FI Receipts will contain the date of issue, the FI beginning and ending numbers, the Family ID and Participant ID(s) and the months of issue (Attachments 9 &10). The Paper Receipt will be used to collect the Endorser or Authorized Representative signature. This receipt will also be used to document the User ID and Staff Name when Mailing is selected. Paper receipts are to be maintained in the participant’s file in accordance with record retention policies.
    c. Paper Income Verification receipts will contain the clinic number, Family ID, and the verification statement (Attachment 11). The paper receipts will be used to collect the staff signature. Paper receipts are to be maintained in the participant’s file.
    d. PDF forms with the digitized signatures will be maintained in the MIS; however paper PDF forms shall be printed if the digitized signature pad is not functioning properly and are to be maintained in the participant’s file. If the MIS is down entirely staff shall use the attached (Attachment 12) paper Rights and Responsibilities form for the participant and staff signatures. This form is to be

maintained in the participant’s file. Paper pdf forms with digitized signatures do not have to be maintained in the participant’s file but it is recommended to keep a copy in the file as a backup in case the system is down.

e. Digitized Signature records will be part of the electronic FI record. To view a digitized signature for an FI, staff will access the FI and Archive FI Lookup Screens. Staff with security access will click the Digitized View button to display a view of the collected signature for this FI.

f. Should the digitized signature pad demonstrate operational failure, implement the following steps:

g. Use the paper forms appended to this policy.

h. Complete the entire forms with the appropriate signatures and date the form.

i. If Endorser/Proxy refuses to sign the paper register, FIs must not be given.

j. All information relative to the operational failure of the digitized signature is to be documented in the MIS and the form placed in the chart file.

k. MIS and Vendor Assistant Security

1. Local Agencies shall designate a Security Officer and a backup who are equally responsible for security issues. These individuals shall be responsible for completing the WIC MIS System Request Form (Attachment 15).
2. The PA WIC Program and the MIS and Vendor Assistant systems are required to comply with all Commonwealth security policies. This applies to all personnel who have access to an account on any system that resides at a facility that provides WIC services and is connected to the Commonwealth network.
3. Staff shall only access the MIS and Vendor Assistant systems under their own user IDs and passwords. Staff shall NOT add, edit or delete information in the MIS or Vendor Assistant system if the system session was initiated by another user.
4. User IDs and passwords are an important aspect of computer security. As such, all Commonwealth employees, contractors, subcontractors, grantees and any other temporary staff person or person(s) with access to the Commonwealth systems are responsible to maintain the security of their user IDs and passwords.
5. All Local Agency staff shall sign the confidentiality form (Attachment 13) each year at their employee performance review. The form shall be kept in the employee’s folder and will be reviewed during the state program review.
6. A formal request to obtain access to the MIS system for new employees, reinstated employees,changes to MIS security for employees, or inactivation of employees shall be submitted to the State Agency by entering an incident

report ticket and attaching the WIC MIS System Request Form (Attachment 14 & 15).

a. When entering the incident report select the following:
   i. Category = Apps WIC
   ii. Type = Security
   iii. Item = add, modify or remove

b. State Agency staff will authorize the staff person in the system and send out an email informing the Local Agency of the authorization.

c. A retailer who wishes to access Vendor Assistant must register to use the system via the Vendor Assistant website, and the system will automatically process the request.

d. Security officers shall submit the WIC MIS System Request form to inactivate MIS user IDs no later than 48 hours after staff have terminated their employment.

e. State Agency staff shall not delete clinic memberships of inactivated user IDs so that the staff’s name and MIS user ID are kept in the histories of records and comments.

f. Local agencies must maintain a typed list of users and their security levels assigned to them in the MIS system. This list will be reviewed during the state program review.

14. Creating User IDs

a. MIS system user IDs should begin with the letter W; include the Agency number, clinic assignment and two additional characters. For example; W30001AB would indicate the user was from Agency 30, Clinic 001.

b. MIS system user IDs shall be inactivated after 120 days of non-use in cases other than termination.

c. Temporary MIS system user IDs should begin with the letter W; include the Agency number; then the letter T and the first four (4) letters of the person’s last name. For example; W97TMART.

d. For vendor users, Vendor Assistant user IDs are email addresses as entered by the users themselves during registration. For State Agency staff, user IDs must be entered by a system administrator and are the users’ cwopa account email addresses.

15. Creating and Resetting Passwords

a. Security Officers will assign any reactivated MIS system password as “changeme” for all users. At their initial sign on, each user will be required to personalize their password.

b. MIS system passwords must be changed at least once every sixty (60) days. MIS system passwords will be inactivated after thirty (30) days of non-use in cases other than termination.
c. Passwords must be kept confidential and should not be written down or inserted into e-mail messages or other forms of electronic communication.
d. MIS system passwords must be at least eight (8) characters long, contain both upper- and lowercase letters (e.g., a-z, A-Z), and have at least one (1) digit (e.g., 0-9) or punctuation character (e.g., !@#$%^&*()). MIS system passwords must not contain a word in any language, slang, dialect, jargon, etc. or be based on personal information, names of family, or other information readily available to others.
e. Vendor Assistant will automatically generate a password for vendor users.
f. System administrators will establish a Vendor Assistant password for State Agency users consisting of the capitalized first letter of the user's first name followed by his/her last name in lowercase, followed by the "pound" (#) sign, followed by the number one (1).
g. At any time should you suspect that your MIS system password has been compromised, report the incident immediately to your Security Officer, the State Agency or complete an Incident Report requesting your password be reset.
h. At any time should you suspect that your Vendor Assistant password has been compromised, log into the system and click "Change Password" on the menu on the left. Then, fill in the information on the form and click the "Change Password" button.
i. Vendor Assistant passwords must contain upper- and lowercase alphabetic characters (e.g., a-z, A-Z), digits (e.g., 0-9), and punctuation characters (e.g., !@#$%^&*()). Vendor Assistant passwords must be at least eight (8) characters, but no more than 15 characters, long.

16. Password Protection Standards

a. All passwords are to be treated as sensitive, confidential Commonwealth information.
b. Do not share passwords with ANYONE.
c. If someone demands your password, refer them to this policy or have them call the State Agency or your Local Agency Security Officer.
d. Do not write your password down, post it on your PC, or store it in your office.
e. Do not reveal your password over the phone.

1. Do not use the same password for the WIC MIS or Vendor Assistant systems as for other non-WIC access systems (e.g., personal ISP account).

2. MIS system passwords will be locked after three (3) consecutive failed log-on attempts and will require administrator-level access to unlock them. In addition, once a user is logged in, the MIS system will be locked after fifteen (15) minutes of inactivity, requiring the user to re-enter the password to regain access to the system.

Attachments:
1. Directions for completing the Data Equipment Request
2. Data Equipment Request Form
3. Directions for completing the Transfer Equipment Request
4. Transfer Equipment Request Form
5. Directions for completing the Equipment Physical Inventory
6. Equipment Physical Inventory Form
7. Directions for the laptop log
8. Laptop Log
9. Instructions for Filling Out Handwritten Register Form
10. Handwritten Register Form
11. Paper Income Verification Form
12. Paper Rights and Responsibilities Form
13. Confidentiality Form
14. Direction for WIC MIS System Request Form
15. WIC MIS System Request Form

Reference(s):
1. P&P 3.03 Documentationof Expenses
2. Commonwealth of PA ITBSEC007 – Minimum Standards for User ID and Passwords
3. USDA/FNS Handbook 701, July 2001
4. WIC Regulations: 7 CFR Part 246.
5. WIC Regulations: 7 CFR Part 246.2.
6. USDA Memo dated July 15, 2004 SFP-04-088
7. Commonwealth of PA ITBSEC006 - Electronic Signature Policy

Policy and Procedure Status:
1. This P&P supersedes P&P Number 8.01 dated April 23, 2009.
2. This P&P supersedes P&P Number 8.02 dated March 11, 2014.
3. This P&P supersedes P&P Number 8.03 dated March 14, 2008.
4. This P&P supersedes P&P Number 8.04 dated June 11, 2012.
5. This P&P supersedes P&P Number 8.05 dated August 31, 2012.