

Subject: KWIC Security

Effective Date: October 1, 2015

Revised from: October 1, 2014

Policy: Individuals, including WIC staff and State Agency employees, involved in the WIC certification and check issuance process, are responsible for the safeguarding of WIC Program client information and the physical equipment used in the administration of the program.

Procedure:

WIC clinic IT support staff must follow the measures outlined in the table below regarding physical, network, operating system, and application levels of security.

Layer	Security Practices Implemented
Operating System	<ul style="list-style-type: none"> • Apply latest service packs and security patches in a timely manner. • Disable all unnecessary services. • Enable strong password policies at the Local Agency level. • Install and automatically update anti-virus protection.
Application	<ul style="list-style-type: none"> • Require unique logon for all KWIC application users. • Enable strong application password policies. • Enable access on a screen-by-screen basis using application groups and role permissions.

Clinic Specific Issues**1. Physical Site**

Local Agencies are required to exercise physical security of KWIC equipment, data and supplies. Buildings containing WIC equipment should be locked and secured outside of regular business hours.

2. Inventory Control

Magnetic ink toner cartridges and check stock must be stored in a locked, secure location. Staff should contact KWIC Support to order MICR toner and check stock. These items will be distributed in limited quantities to replace exhausted cartridges and check stock at the local clinics.

3. Portable Equipment

Laptop computers should be fitted with locks designed for laptops, and secured to a desk whenever possible. Unattended laptops should be locked to a desk or similar immovable object, or stored in a locked cabinet or room. Laptops should not be left in vehicles unless locked in the trunk out of view. Laptops should be protected from excessive heat and cold. Portable check printers should be secured in the same manner as laptops.

Subject: KWIC Security

4. Data Security and Confidentiality

As part of training, all clinic personnel will be trained in confidentiality requirements and steps to protect unauthorized disclosure. Staff will be trained to lock the computer whenever leaving their desks.

It is imperative that access to client data be closely managed to conform to State, Federal, and contractual requirements for confidentiality.

The KWIC system tracks the staff ID associated with each client contact, including issuance of checks and completions of client certifications.

5. Virus Protection

All workstations used for KWIC must have up-to-date virus protection software installed. The software must be configured to automatically update itself on a regular basis.

Users are required to follow established policies prohibiting downloading and/or installing unauthorized applications or data onto WIC computers. Staff should comply with KDHE and local agency policies regarding downloading approved applications and virus screening.

6. Application Security

WIC staff must enter a user ID and password before gaining access to the Client Services application. The role permission assignments will be maintained by the State WIC office.

Clinic staff are designated to a particular role permission by the State WIC office, who regulates access to the application on a screen-by-screen basis. Access levels for each user ID shall be limited to the screens necessary to fulfill that staff's responsibilities. Each staff shall have a unique user ID assigned. User IDs and passwords may not be shared under any circumstances. The KWIC system has an administrative report that shows all users authorized to perform specific functions.

The application security controls are flexible enough to accommodate staff with multiple roles, which is typical for small clinics. State Agency staff creates role permissions and assigns screen access to the role permission. As an example, the State WIC staff can create a role permission called "Clerk/Administrator", which could be used by small clinics where the clerk has more responsibility and authority than normal.

Passwords must be entered manually. The KWIC application forces a password change every 90 days and the new password must be dissimilar from the previous password.

KWIC Help Desk staff are able to change passwords for the KWIC application. The creation of new user accounts and the inactivation of existing accounts are completed by KWIC Help Desk staff upon request by State Agency staff. This process ensures that each KWIC user has only one valid user account. KWIC Help Desk staff will assign the user to specific role permissions and assign access privileges for the user. The KWIC system requires that users change the temporary password at the time they first log onto the system.

Subject: KWIC Security

7. Network Security

WIC staff must enter an account name and password to gain access to the Local Area Network (LAN) at the clinic. LAN user accounts and access privileges will be managed locally. Clinics that have existing networks and local IT support are responsible for managing their own local network security.

8. Internet Connectivity

Clinics with a LAN, Internet connection and local IT support can freely access the Internet according to the policies and procedures established by the local agency.

It is outside the scope of the Kansas WIC Program to provide support for full Internet access for clinic staff.

9. WIC Checks

Blank check stock is stored at WIC clinics. Also, MICR-enabled printers are used to print checks on a daily basis.

Since most check printers will be printing for several workstations, checks will have a tendency to “pile-up” in the output bin of the printer. For this reason, the check printer should always be within the sight of a local WIC staff member.

To further minimize the risk of fraudulent printing or theft of checks, the following steps are recommended:

- The MICR enabled printers should be closely monitored. The printer should be placed in a location removed from waiting areas and high traffic areas where possible.
- MICR toner cartridges and blank check stock should be securely stored and usage tracked.