1.26 Security Policy

POLICY:

State and local agencies are responsible for the security of all ADP projects being developed and operational systems involved in the administration of FNS programs. State agencies shall determine appropriate ADP security requirements based on recognized industry standards of standards governing security of Federal ADP systems and information processing.

SCOPE:

All State and Local agency WIC personnel will adhere to the policies and procedures herein described as well as those already established by the State of West Virginia Office of Technology Policies: http://www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

- Information Security Policy
- Internet Usage Policy
- Email Use Standards
- Acceptable Use of Portable and/or Wireless Devices

along with Chapter 61, Article 3C. West Virginia Computer Crime and Abuse Act., http://www.legis.state.wv.us/wvcode/ChapterEntire.cfm?chap=61&art=3C

PROCEDURE:

The State Agency (SA) will maintain a program for conducting periodic risk assessments to ensure that appropriate, cost-effective safeguards are incorporated into new and existing systems. A risk assessment shall be performed whenever significant system changes occur.

The SA will review the ADP system security of 20% of all WIC clinic sites on a biennial basis. The review shall evaluate physical and data security, operating procedures, and personnel practices. The SA will determine compliance with requirements and provide a written summary of all findings to both the local agency and FNS after the completion of the ADP System Security Review. The SA will submit a plan of corrective action to the Local Agency with dates of scheduled milestones, when completed, will correct any security weaknesses.

The State Agency will provide one copy of all IT Policies initially to each local clinic site. These policies will be kept on-site for review and new staff training. The Local Agency will be notified of changes to the IT Policies on the web sites. It will be the responsibility of each local clinic site to update these separate policies.

A. Administrative/Management Security Controls

The SA will delegate a staff member who will act as the WIC Security Officer. The roles of the WIC Security Officer are outlined under the Personnel Security section of this policy. The WIC Security Officer will track all system breaches and monitor and test for vulnerability of security safeguards at irregular intervals but at least once a year.

B. Computer Security Controls

1. Access Control

Controls are to be established by the SA to prevent unauthorized persons from reading from and writing to programs and data files. The SA and the Local Agency (LA) Director will submit to the WIC Security Officer a Network Logon form for all staff that leaves

employment immediately. The LA Director will also submit a new form for all new hires. Staff under no circumstances shall share network/Crossroads/MMIS/E-WIC passwords and logon ID's. Invalid login attempts will lock user out of the network after five (5) attempts. Crossroads will lock out the user after two (2) unsuccessful attempts. For security reasons, all passwords cannot be seen. The network automatically locks the computer after 5 minutes of inactivity. All staff are instructed to lock computer screens whenever leaving their computer unattended. Should a particular PC be used by multiple persons within the clinic site, each person must log out prior to another person's use of the PC. The WIC Security Officer shall maintain a current list of all system users.

2. Identification and Authentication

Both the WIC network and the Crossroads application use the same network ID and password. Crossroads users are added to the application with their network ID's and given the appropriate roles to the clinics they need access to. Network IDs are approved and processed by the WIC security as stated above. The WIC Helpdesk adds the roles for the user in Crossroads providing for a separation of duty at the state office.

Wide Area Network

< All sensitive telecommunications equipment will be guarded from unauthorized physical access.
< All connections from remote systems will be subject to authentication. In addition, all remote connections to WAN equipment will display the following banner:

****

WARNING: This system is for the use of authorized clients only. Individuals using the computer network system without authorization, or in excess of their authorization, are subject to having all their activity on this computer network system monitored and recorded by system personnel. To protect the computer network system from unauthorized use and to ensure the computer network system is functioning properly, system administrators monitor this system. Anyone using this computer network system expressly consents to such monitoring and is advised that if such monitoring reveals possible conduct of criminal activity, system personnel may provide the evidence of such activity to law enforcement officers. Access is restricted to authorized users only.
Unauthorized access is a violation of state and federal, civil and criminal laws.
Department of Health & Human Resources WIC.

****

Local Area Network

< Policies will be in place on all PCs connected to the LAN requiring validation from the network server in order to access Windows.
< All SA and LA Clinic personnel are required to have a unique network logon ID.
< Passwords for logon IDs will expire and must be changed every sixty days.
< Any network logon account unused for ninety days will be disabled.

CROSSROADS

WIC Clinic and State office staff will have the same USER ID as the network as stated previously.

< Local Agency Directors or their designee will instruct the WIC Security Officer and WIC Help Desk where the user will be working and what duties they will be performing. After the WIC Security Officer approves the network login and OT has completed the Network Login setup, WIC Help Desk will add the user to the Crossroads application.

< Local Agency Directors or their designee is also responsible for making sure people are deleted from the system by filling out an OT Network Deprovision form on line and assigning it to the WIC Security Officer for approval. This shall be performed within 24-48 hours or less after personnel leave employment.

< Crossroads passwords are encrypted and cannot be seen on the screen. Passwords also expire every sixty days at the same time that the network passwords expire. Crossroads has a link to the active directory to verify passwords. So the passwords expire and are the same for both systems. Crossroads does have a separate login screen but uses the network login and passwords information. If a user mistypes, the password twice logging into Crossroads, the system automatically also locks the network password.

< When staff leave their desks for any length of time, they should lock their computer screen.

3. Audits

Audits should be available in the system to track problems and look at security issues within Crossroads

Crossroads has security files, automated error logs, time and date stamps on records.

< User IDs are assigned to records automatically to record who is doing a particular function in Crossroads. These areas are Income and Residency, Blood Work, Height and Weight, and Food Package Assignment, risk assessment, Benefit Issuance, Care Plans, and Nutrition Education at a minimum.

< Security files are kept that include when passwords are to expire, number of unsuccessful attempts

< The security file also limits what a user can do depending on flags that are set when they are added to the system. If a function is not permitted to the user, the menu will be faded and not accessible for that function.

< A file is also available to track logon error and violations.

4. Configuration Management

The Crossroads System Manager, SA Equipment Coordinator and MIS Project Leader must approve every change made to documentation, hardware and software. As new equipment is added to sites, a ghost image is made which is copied to all new PC equipment ensuring that all new PCs will set up exactly the same including all files needs to run the Crossroads application.

Computer Equipment Purchases

All computer equipment purchases will be handled through the WV WIC program state office. Any purchase of automated data processing equipment and software must have prior SA

approval. See WV Policy & Procedure 6.11.
State Requirements

- < Any purchase exceeding $500.00 and being less than $5000.00 requires that three verbal bids be obtained. Documentation verifying the bids must be provided.
- < Any purchase exceeding $5000.00 and being less than $10,000.00 requires the use of state approved vendors and a minimum of three written bid quotes.
- < Any purchase exceeding $10,000.00 must be placed on the State's Purchasing Bulletin Board and requires a signed bid summary from WV Office of Technology and WV DHHR MIS.
- < Any invoices not meeting the above criteria will be rejected by the WV State Auditors Office.

Federal Requirements

- < The SA will provide a five-year plan which lists ADP equipment at both the SA and LA level which will give purchase date and anticipated replacement date. The five-year plan will also include anticipated costs associated with the replacements.
- < Purchases not listed on the five-year plan and greater than $100,000 will need prior USDA approval.
- < See FNS Handbook 901

C. Communication Controls

Physical Security

Clinic Sites

All sensitive networking equipment, to include servers, routers, and switches, will be located in the most secure area of the clinic. If it is necessary that the equipment be located in a room used to serve clients, the equipment will be placed in a manner that prohibits access. This will be accomplished by storing the equipment in a protective cabinet or restricting client access to the area. The LAN file server is never to be used as a workstation. Policies are placed on file servers to allow access only by the Network LAN Specialist.

State Office

Networking equipment and servers for state personnel is located in the computer room at Bldg6 of the WV State Office Complex.

In addition, both the WIC state office and LA clinics will follow the West Virginia State IT Policy - Physical and Environmental Security, Reference I, Policy 12.0.

D. Information Security Controls

1. Data/File Protection – The following guidelines will be followed by both the SA and LA staff to ensure proper data/file protection:

Backup and Recovery

State Office

- All servers holding information pertinent to WIC will perform full backups nightly via the network to an external storage device.
- In case of a data loss, or hardware failure in a file server, a full backup will be restored by WV Office of Technology staff.
- All servers will be connected to a power conditioning UPS in order to prevent data loss and hardware damage.

Clinic Sites

- All file servers located at WIC clinics will be backed up nightly with a 30 day retention.
- In case of a data loss, or hardware failure in a file server, a full backup will be restored by WV Office of Technology Staff
- All servers will be connected to a power conditioning UPS in order to prevent data loss and hardware damage.
- Files should not be saved to the Clinic PC's as they are not backed up.

2. Data/Software Backup

Application backups are also being completed for the Crossroads servers by WV Office of Technology back up procedures.

3. Security Training

All Local Agency staff is required to have mandatory online information security awareness training performed annually. This training is provided by WV Office of Technology annually and is provided online.

E. Personnel Security Controls

1. Organization

Responsibilities in this area include that of the SA and MIS Department to hire and train personnel in proper security procedures. WIC/MIS shall hire and maintain certain levels of personnel with differing roles and responsibilities. Staff shall always have someone who can back them up if the need arises. Personnel shall be assigned certain roles and responsibilities according to their skills.

The SA will establish the roles and responsibilities of MIS Personnel. The WIC SA and LA Users will adhere to all current state procedures and outlined roles and responsibilities as outlined in Reference I, Policy 3.0 - Management and Staff Responsibilities.

The SA will maintain and update as needed a set of roles and responsibilities for all MIS staff. This will be done on a periodic basis, probably during Employee Evaluations and reviews. Once established, these responsibilities should not be modified unless job duties change. WIC/MIS Project Leader and WIC Equipment Coordinator report to DHHR/MIS supervisory staff and receive direction from WIC State Agency Administrative staff. The Helpdesk Analyst and Crossroads Project Manager will report directly to WIC State Agency Staff.

2. The Current WIC/MIS positions and responsibilities are as follows.

a) **WIC Security Officer**

- Approve and Maintain Local Agency User Sign-on's to the LAN.
- Developing the ADP Security Policies/Plan along with the WIC/MIS Project Leader and the Crossroads Project Manager.
- Investigate security breaches of any type recommending emergency procedures when deemed necessary. Informing MIS and WIC administration of problems as necessary.
- Monitor adherence to WVOT and WVDHHR Security Policies.
- Assist in contingency planning for emergencies at the local level.
- Review biennial security review of 20% of WIC Sites completed by the WIC Equipment Coordinator according to the review policy.
- Maintain a list of all Logon ID's issued and what locals they are assigned to and their duties.
- Coordinate with the Field PC Technician, the inventory of WIC computer equipment.

b) Crossroads Project Manager

- Supervise Helpdesk Analysts and EBT coordinator positions
- Coordinate all equipment and Crossroads related functions with local and site staff.
- Coordinate with MIS Supervisory staff the duties of the WIC Equipment Coordinator and give directions to the staff member.
- Assist the trainer in developing Crossroads Training.
- Developing the ADP Security Policies / Plan along with the WIC/MIS Project Leader and the WIC Equipment Coordinator.
- Assist in contingency planning for emergencies at the local level.
- Gather Site Surveys and WV WIC Program Site Description form every year from local sites according to policy.
- Contact person for local site offices that are moving.
- Oversee Equipment Inventory practice of field equipment.
- Gather work requests from sites for equipment repairs

c) **MIS/WIC Project Leader**

- Develop the Security Policies/Plan with the Crossroads Project Manager
- Act as WIC Security Officer
- Determine system needs and modifications to the Crossroads System and present them to the Crossroads User Group along with the Crossroads Project Manager
- Coordinate System Distribution
- Solve Complex processing problem with nightly batch processing, as needed.
- Work with WIC Admin Staff and Field Users to determine needs.
- Determine needs associated with new federal regulations.
- Provide needed reports to the Regional Office along with the Crossroads project Manager.
- Give direction to WIC Equipment Coordinator and Helpdesk Analysts
- Oversee the overall function of all MIS Processes
- Ensure that sites are able to serve clients

- Coordinate all EBT processing and daily redemptions reconciliation
- Coordinate and process ACH payments to the Cap Formula Warehouse.
- Develop Crossroads reports as needed
- Run reports for the 798, rebates and caseload monthly

d) WIC Equipment Coordinator

- Ensure all servers are successfully backing up on an appropriate level.
- Create Telecommunication Change Requests for phone and WAN line changes.
- Coordinate equipment purchases along with MIS to post requested computer purchases for approval by WV Office of Technology.
- Coordinate moving of computer equipment and network lines at WIC local offices that are moving.
- Coordinate the replacement of computer equipment in field offices and state office with the Office of Technology.
- Coordinate repairs for equipment that is under warranty with vendors providing the equipment with OT field staff.
- Add and update software to PCs as necessary.
- Ensure that inventory records are kept up-to-date.
- Coordinate maintenance with all sites.
- Match inventory records with on-site inventory on a biennial basis.
- Assist in problem resolution with Autodialer
- Revise the Five Year Equipment Replacement Plan and see that goals are met accordingly.
- Request OAF(Operational Adjustment Funding) funding for equipment to meet the Five Year Plan.
- Coordinate with eRecycle and surplus on how to dispose of computer hardware following department guidelines ensuring proper data encryption and/or destruction.

e) **Help Desk Analyst**

- Answer Help Desk calls from local sites and resolve problems over the phone.
- Resolve and monitor Autodialer activities.
- Train users on solving Crossroads Problems over the phone.
- Test new version of Crossroads according to the release management notes.
- Assist Crossroads Project Manager in determining errors and entering JIRA tickets for Crossroads UAT and Production Problems.
- Be available to assist on Crossroads Design calls, as requested
- Assist WIC Crossroads Manager and MIS Project lead as needed
- Maintain user rights and roles within the Crossroads System and E-WIC system.

3. Separation of Duties

Within the SA, separation of duties is accomplished in the following manner: WIC IT Staff are separated into different levels of responsibilities depending on their civil service classification. WIC Project Manager and WIC MIS Project lead with have will have separate responsibilities from The WIC Equipment Coordinator and Help Desk Personnel. Both units may backup the other unit, when necessary due to illness, vacations or vacancies.

The WIC Security Officer will approve network logon requests received from the LA Directors. These will then be completed by WV Office of Technology staff. The WIC Crossroads manager will oversee the roles that are available within Crossroads. The WIC Help Desk Staff will add/maintain users within Crossroads and give them the roles and site access as needed in Crossroads.

Software Development

All modification request are presented to the Crossroads User Group for approval. Once approved, the Crossroads Maintenance and Enhancement contractors will create the system design for approval and implementation.

4. Personnel

Each SA/LA employee must sign a Confidentiality Statement upon their hiring. This statement extends to participant records, databases, and the release of information. Reference II draft IT policy 0504 also addresses the issue of Background Investigations and Employee Confidentiality Statement.

It is also the responsibility of the SA and LA Director to brief all new employees on the Security Policies in effect. Upon termination of employment, personnel must turn in to the Security Manager/LA Director all identification cards, keys, programs, data files etc. in their possession. SA and LA Director must interview and emphasize to each terminated employee their continuing responsibility to maintain the privacy and confidentiality of State data.

SA staff will be briefed on Emergency Preparedness annually, which will include fire evacuations and procedures to follow in the event of a bomb threat. The SA staff will follow regulations as set forth in Reference V.1 & Reference V.2 Bomb Threat Checklist.

SA and LA personnel will abide by the following System Usage guidelines
E-Mail Usage

< Every WIC staff member will have their own personal email account. In addition, there is a clinic email for each clinic site. This email may be accessed by multiple people within the clinic. Clinic personnel will check for new messages a minimum of once a day for the clinic email.
< Microsoft Outlook provided by the Office of Technology desk will be the only e-mail programs installed on WIC PCs. Use of Internet E-mail services such as Hotmail is prohibited.
< If a message is received that is designated as “Critical”, clinic personnel will open the message in a minimum of two working days.
< All WIC state office and clinic staff will abide by the Email Use Standards Policy mentioned previously.

Internet Usage

< All WIC personnel will adhere to the Internet Usage Policy and Information Security Policy mentioned earlier.

Other Software

- < Microsoft Office is installed on all clinic PC's
- < Security Policies will be placed on all PCs preventing the installation of software by unauthorized users.
- < All software installed on WIC PCs will be purchased according to the Computer Equipment Purchases Policy. See West Virginia Policy & Procedure 6.11.
- < The SA will maintain licensing information for all software.
- < Any additional software must be installed by WV OT staff and approved by the WIC Office.

F. Physical Security Controls

1. Access Control

Physical access to WIC sites will be maintained.
Facility will be locked at all times when authorized personnel are not present.
SA/LA personnel shall wear name badges at all times.
Unauthorized individuals shall be escorted at all times by LA/SA staff.
If access is via an electrically controlled system, a determination must be made if it can be operated by standby battery power or overridden by an accessible key.

2. Equipment Security

WIC Equipment Coordinator will maintain an inventory of all ADP equipment with serial numbers, locations and maintain records. This information is also to be kept by the LA which is updated and submitted to the SA biennially per State WIC Policy & Procedure 6.15.
File servers will be placed in limited access area if possible. If this is not feasible, servers may be stored in a protective cabinet or by restricting client access to the area.
Proper equipment maintenance/warranty coverage will be maintained for all PC equipment.
All computer equipment with memory stored inside hardware must be picked up by WV eRecycle team. WV eRecycle will ensure that all data has been wiped from the device prior to surplus/retirement.

G. Environmental Security Controls

A West Virginia WIC Program Site Description Chart (Reference VI) will be completed/updated for each site administered by each Local WIC Agency by **July 1** of each year. This survey will be used for any **potential** site when relocating clinics. All site surveys will contain emergency contact numbers with a primary number and a secondary phone number for each site.

The Local Agency will complete the Local Agency/SA Security Survey (Reference VII) by **July 1** of each year.

Environmental Security - (See Reference I - State of WV Information Security Policy 4.4 Physical & Environmental Policy)

1. Water Damage

Local Agencies will consider environmental issues that may affect clinic and equipment operations when choosing a new clinic site. Potential sites should be examined to determine the probable effect from damage or destruction of contents, interruption of electric power and

communications, lack of access to the building due to water/flood related issues.

In addition to the overall effect of natural flooding, examine the flood damage potential from all causes. Evaluate the location/future location of computer equipment within the building. (A basement location is potentially the least desirable location). Inspect the ceiling above ADP hardware areas for previous water leakage stains

2. Fire Exposure

Review fire emergency procedures with staff, assigning individual responsibilities in the event of fire and ensure staff knows the location of all fire extinguishers. Local fire department may be able to provide training in these emergency procedures.
Place portable fire extinguishers strategically in clinics with location clearly marked.
If building is equipped with automatic fire extinguishing systems, determine its adequacy and readiness.
Determine the location of smoke detectors.

3. Natural Disaster/Housekeeping Program

Determine if the building and equipment are properly grounded for lightning protection.
Keep computer area free of accumulated papers/trash. This would include refraining from stacking papers, books, handouts on and around the CPUs. These items prohibit the free flow of air that the CPU needs to keep the equipment from overheating.
Food and drink must be kept away from computers and their peripherals.
Install surge protectors to prevent electrical fluctuations
To prevent destruction of data, the LA staff will notify SA should the UPS malfunction and become inoperable.
The SA will secure LA equipment that is covered by a three-year warranty to provide equipment maintenance as well as provide a field tech to do routine PC maintenance.
Ensure that backup tapes are stored in fire resistant box.

4. Contingency Plan

Contingency plans are to protect PC equipment and its users against unacceptable loss. Proper procedures must be in place in the event of weather related emergencies and sudden power losses. The SA will identify those applications that must be run immediately, those that can be delayed, and those which can be postponed indefinitely or performed in another manner.

Daily backups are performed on the file servers and on the communication stations of each site.

Disaster Recovery Exercises will be conducted yearly for the IS&C mainframe to ensure continued operation in the event of an emergency. See Reference VIII.

H. Procedures for WIC Biennial Security Review

The objective of the biennial security review is to perform a network security assessment of the West Virginia WIC Program. The project will involve work being performed on-site at county WIC clinics as well as remotely gathering information on computer systems prior to the on-site visit for corrective

action and discussion with the appropriate Local Agency WIC directors. Additionally, a physical safeguards assessment will take place during the on-site visit.

Security reviews consisting of WIC networks will be audited using remote security software in order to detect, interrogate, test for weak passwords, and report on well-known services of identified WIC computers that are network-connected. Scans will occur one week prior to the scheduled on-site security review, and any findings that cannot be corrected remotely will be addressed during the on-site visit. WIC computer users will not be aware of scans, nor will the security scans affect WIC computer operations.
Also, prior to the on-site visit, information will be gathered about WIC user accounts. Reports of user account inconsistencies, disabled, inactive, never used accounts, will be run one week prior to the scheduled on-site security review. Findings will be discussed with the appropriate Local Agency Director and corrected.

REFERENCES:

1. State of West Virginia Information Security Policies
2. WV DHHR Information Technology Policies and Procedures
3. Chapter 61, Article 3C. West Virginia Computer Crime and Abuse Act
4. Diamond Emergency Preparedness Guide
5. FNS Handbook 901

ATTACHMENTS:

1. West Virginia WIC Program Site Description Chart
2. Local Agency Security Survey