

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 and the Department of Health & Human Resources which include the West Virginia Information Security Policy, http://www.state.wv.us/itc/std_cvr/policies/security.htm; West Virginia Department of Health and Human Resources Security Policies, <http://intranet.wvdhhr.org/Policies/IT/index.htm>; and Chapter 61, Article 3C. West Virginia Computer Crime and Abuse Act., <http://intranet.wvdhhr.org/policies/IT/613c.htm>

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 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 separately from the Policy and Procedure Manual. 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. This person will report to the DHHR/BPH Security Manager. 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 employ immediately. The LA Director will also submit a new form for all new hires. Staff under no circumstances shall share network/STORC passwords and logon ID's. Invalid login attempts will lock user out of the network after five (5) attempts. STORC will lock out the user after three (3) unsuccessful

1.26

Security Policy

attempts. For security reasons, passwords to both the network and STORC sign-in screens cannot be seen. A screen saver has been developed in STORC which when activated, will not allow reentry until a password is again inputted into the system.

All staff are to use this feature 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 STORC application require both a unique logon ID and password. All WIC personnel will also adhere to the State of West Virginia Network Security Policy. See Reference I, Policy 5.0 & 13.0. In addition, all staff must adhere to the guidelines listed in the STORC User's Guide and for those working as Competent Professional Authority (CPA's) the West Virginia WIC Program Policy and Procedure Manual Policy 2.03 and 2.19. In addition, the following also applies to the WAN, Network and STORC application access.

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 thirty days.
- < Any network logon account unused for ninety days will be disabled.

The following banner will displayed upon access to all PCs:

This system is for authorized users only. Users of this system must abide by DHHR policies, procedures & standards. All system use is subject to monitoring & recording by authorized personnel. Misuse may lead to disciplinary action and/or prosecution.

STORC

WIC Clinic and State office staff will have a separate user ID for STORC. This is in addition to he LAN Logon ID's mentioned previously.

1.26

Security Policy

- < Local Agency Directors or their designee will add the user to STORC and give them the appropriate system rights for their job duties.
- < Local Agency Directors or their designee is also responsible for making sure people are deleted from the system in a timely manner after personnel leave employment.
- < STORC passwords are encrypted and cannot be seen on the screen or in the database. Passwords also expire every thirty days.
- < STORC User ID's should never be shared with other staff. Staff should also use their own ID's when in STORC.
- < When staff leave their desks for any length of time, they should either get out of STORC and go to the desktop or Press F9 to bring up the STORC Screen Saver.

3. Audits

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

STORC uses Initials in critical areas, security files, automated error logs, time and date stamps on records, and nutrition encrypted stamping of the progress notes in the system.

- < Initials in critical areas - STORC requires that initials be placed of the person doing the particular function within the system. These areas are Income and Residency, Blood Work, Height and Weight, and Food Package Assignment.
- < Security files are kept that include when passwords are to expire, number of unsuccessful attempts, encrypted password.
- < Whenever a record is completed, a history record is created showing when the change took place and who the last user to complete the record was. These fields are also found on all major database records, such as draft, client, progress note, client, diet, nutrition education, etc.
- < When a nutritionist completes a progress notes, they must electronically stamp the note by pressing a function key. This then assigns this note to the nutritionist who was signed on to STORC when the progress note was completed.
- < 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 SA Network Specialist 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 to a CD which is copies to all new PC equipment ensuring that all new PCs will set up exactly the same including the most recent version of STORC.

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.

1.26

Security Policy

- < Any purchase exceeding \$10,000.00 must be placed on the State's Purchasing Bulletin Board and requires a signed bid summary from WV IS&C Office.
- < 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 \$25,000, will need prior USDA approval.

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 350 Capitol Street. See Reference IV, Memorandum of 4/24/2000 which describes in detail Computer Room Security/Access.

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 WIC help Desk and WVDHHR MIS staff.
- < All servers will be connected to a power conditioning UPS in order to prevent data loss and hardware damage.

1.26

Security Policy

Clinic Sites

- < All file servers located at WIC clinics will be equipped with internal AIT tape backup devices. All servers will automatically perform a full backup every Monday and differential backups nightly Tuesday through Friday.
- < Clinic staff will be provided three backup tapes for each server. Tapes will be rotated every Monday. Tapes not currently in use will be stored either off site or in a fire resistant storage container.
- < One PC located at each WIC clinic will be equipped with an internal tape backup device. This PC will automatically perform a backup of STORC data weekly.
- < Clinic staff will be provided backup tapes and will rotate the tapes every Monday. Tapes not currently in use will be stored either off site or in a fire resistant storage container.
- < In case of a data loss, or hardware failure in a file server, a full backup will be restored by WIC help desk staff.
- < All servers will be connected to a power conditioning UPS in order to prevent data loss and hardware damage.

2. Data/Software Backup

All new software will be backed up immediately with original distribution diskettes/CDs stored in a fireproof safe. Should software programs be damaged, a restore should be done from the original CD's. Only new media will be used for distribution.

3. Security Training

All Local Agency staff is required to have mandatory online information security awareness training performed annually.

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 personnel shall report to DHHR/MIS supervisory staff and receive direction from WIC State Agency Administrative staff. The PC Tech, Helpdesk Analyst and STORC Project Coordinator will report directly to WIC State Agency Staff.

1.26

Security Policy

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

a) **LAN Network Specialist/WIC Security Officer will:**

Add 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 STORC Project Coordinator.
Investigate security breaches of any type recommending emergency procedures when deemed necessary. Informing MIS and WIC administration of problems as necessary.
Monitor adherence to DHHR Security and IT Policies.
Assist in contingency planning for emergencies at the local level.
Perform biennial security review of 20% of WIC Sites according to the review policy.
Coordinate equipment purchases along with MIS to post requested computer purchases on the bulletin board.
Coordinate moving of computer equipment and network lines at WIC local offices that are moving.

Work closely with MIS WAN/LAN Staff concerning WIC LAN's and communications.
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.
Ensure all servers are successfully backing up on an appropriate level.
Create PC Policies for all PC's in field offices to limit PC misuse.

b) **STORC Project Coordinator**

Supervise Fields PC Technician and give direction to the LAN Network Specialist.
Supervise Helpdesk Analyst position
Coordinate all equipment and STORC related functions with local and site staff.
Train all new local agency on STORC.
Create Telecommunication Change Requests for phone and WAN line changes.
Revise the Five Year Equipment Replacement Plan and see that goals are met accordingly.
Request OAF funding for equipment to meet the Five Year Plan.
Developing the ADP Security Policies / Plan along with the WIC/MIS Project Leader and the LAN Network Specialist.
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
Provide periodic reports to the regional office along with WIC/MIS Project Leader.

1.26

Security Policy

c) **MIS/WIC Project Leader**

Develop the Security Policies/Plan with the STORC Coordinator and the LAN Specialist
Backup LAN Specialist as needed.
Determine system needs and modifications to the STORC and VACE Systems
Assign program modifications to appropriate staff and ensure that testing is performed by all staff.
Coordinate System Distribution
Solve Complex processing problem with nightly processing, as needed.
Work with WIC Admin Staff and Field Users to determine needs.
Coordinate PEDS/PNSS activity with CDC.
Determine needs associated with new federal regulations.
Provide needed reports to the Regional Office along with the STORC Coordinator.
Supervise programming staff
Give direction to Field PC Technician, LAN Network Specialist and Helpdesk Analyst
See that WIC Admin Staff has the needed sign-ons to file reports to the Regional Office.
Oversee the overall function of all MIS Processes
Ensure that sites are able to serve clients
Obtain data from other areas to recover sites as needed.
Create and update all food package assignments with direction from nutrition staff.
Schedule a time to run indexes on servers on a monthly basis.
Obtain all schedule records on a daily basis.
Coordinate all banking activity with FSMC
Coordinate and process ACH payments and resolve problems with FSMC. Vendor staff captures and authorizes payments.
Run BOD and EOD reports, as needed. Mostly performed by Help Desk Analyst and Programming staff.

d) **Field PC Technician**

Replace or repair computer equipment in field offices and state office.
Coordinate repairs for equipment that is under warranty with vendors providing the equipment.
Add software to PCs as necessary.
Ensure that inventory records are kept up-to-date.
Assist the LAN Specialist on all office moves.
Install new equipment as required.
Coordinate maintenance with all sites.
Require that work requests are obtained for work being performed.
Match inventory records with on-site inventory on a biennial basis.
Run network cable as necessary.
Assist LAN Specialist to ensure that backups are being performed on servers on a routine basis.
Backup LAN Specialist as needed in assigning User IDs and maintaining logs of user names and IDs.
Assist in problem resolution with Autodialers.

1.26

Security Policy

e) **WIC Programmers**

Make STORC/VACE modifications as assigned.
Make recommendations as to changes that may need to be made to enhance the

STORC performance and functionality.
Test all changes prior to implementation.
Distribute code as needed.
Train users on solving STORC problems.
Obtain monthly schedules from sites and create weekly log sheets for BOD and EOD to ensure all data is being processed.
Run Nightly Jobs to ensure that data is processed in a timely and accurate manner.
Second on call for Help Desk calls. Help Desk Analyst will take most calls but programmer will pick up overflow and more problematic calls.
Assist Help Desk Analyst on problem calls as necessary.
Refer hardware and policy calls to appropriate people as necessary.
Receive and Send FSMC Data on a daily basis.
Backup Help Desk Analyst on FI inventory and stock.

f) **Help Desk Analyst**

Answer Help Desk calls from local sites and resolve problems over the phone.
Resolve and monitor Autodialer activities in Local Offices.
Do BOD processing at the state office for local offices prior to clinic opening.
Process FI Inventory requests on a daily basis.
Train users on solving STORC Problems.
Monitor weekly backup of communications PCs.
Assist programming and LAN/PC staff as needed.
Reset Network passwords for field offices, as needed.

3. **Separation of Duties**

Within the SA, separation of duties of Information Technology IT personnel is accomplished in the following manner: WIC IT Staff are separated into different levels of responsibilities depending on their civil service classification. LAN/PC personnel will have separate responsibilities from Programmer and Help Desk Personnel. Both units may backup the other unit, when necessary due to illness, vacations or vacancies.

LAN/PC Staff Separation of Duties

LAN Specialist will assign USER IDs and system rights after STORC Project Coordinator and Local Agency Director (or designee) signs off on form
PC/Technician will serve as backup to assigning User IDs for field staff
WIC IT personnel will have their User IDs and server rights assigned by DHHR/MIS Personnel
Local Agency Director or designee is responsible for adding Users to STORC Security.
LAN/PC staff is only responsible for the Network Access

Software Development

All modifications are reviewed prior to work initiation with WIC Admin Staff. Programmers will test their own modifications but other programmers or Help Desk Staff must also test changes prior to distributing code. MIS/Project leader will approve all changes and testing prior to distribution.

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 clinic will be provided with at least one PC with GroupWise installed. Clinic personnel will check for new messages a minimum of once a day.
- < Novell GroupWise provided by the state help 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 WVDHHR Electronic Mail Guidelines and Requirements. See Reference II, Policy 0501 and 0510.

Internet Usage

- < All WIC personnel will adhere to the WVDHHR Use of Information Technology Policy. See Reference II, Policy 0501

Other Software

- < Selected WIC PCs at clinic locations will be installed with word processing and desktop publishing software. WIC help desk staff will install this software.
- < 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

1.26

Security Policy

Equipment Purchases Policy. See West Virginia Policy & Procedure 6.11.

< The SA will maintain licensing information for all software.

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

SA Field Tech will maintain an inventory of all ADP equipment with serial numbers, locations and updated. 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.

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

1.26

Security Policy

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 it's 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.

To prevent loss of data, STORC information is housed not only at the local level, but also at the parent site, the SA and the State operated mainframe. VACE information is also stored both at the SA and at the mainframe. 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

1.26

Security Policy

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:

- I. State of West Virginia Information Security Policies
- II. WV DHHR Information Technology Policies and Procedures
- III. Chapter 61, Article 3C. West Virginia Computer Crime and Abuse Act
- IV. Memorandum - Computer Room Security/Access
- V. Diamond Emergency Preparedness Guide
- VI. West Virginia WIC Program Site Description Chart
- VII. Local Agency Security Survey
- VIII. Disaster Recovery Exercise