

III. INFORMATION SYSTEM (IS)

State Agency: Arkansas for FY 2015

This section, Information System (IS), involves the planning, documentation, security/confidentiality and production of the necessary reports relating to program operations through the utilization of automated data processing services at the State and local level.

A. *System Planning and Operation - 246.4(a)(12)*: describe the procedures for planning, approving and monitoring Automated Data Processing (ADP) goods and services, and any interaction with other statewide ADP operations which may take place, including system costs for services and security.

B. *Participant Characteristics Minimum Data Set (MDS) - 246.4(a)(11)(i)*: All State agencies currently collect all required Minimum Data Set items. Please confirm that your State agency will continue to do so. For the Supplemental Data Set (SDS), which varies by the capacity of State systems, please describe the data items which are reported electronically regarding participant characteristics and whether these items are currently being collected or if there are plans to collect them in the future.

C. *WIC Systems Functional Requirements Checklist - 246.4(a)(8); (9); (11); (12); (13); (14); (15) and (18)*: Describe those functions which are currently incorporated into the IS or which are planned to be incorporated in the future.

III. INFORMATION SYSTEM (IS)

A. System Planning and Operation

1. ADP System Planning

a. The WIC State agency is included in the following comprehensive Statewide ADP plan(s):

- | | |
|---|---|
| <input type="checkbox"/> Title IVa (TANF) | <input type="checkbox"/> Title XIX (Medicaid) |
| <input type="checkbox"/> Title V (MCH) | <input type="checkbox"/> Supplemental Nutrition Assistance Program (SNAP) |
| <input type="checkbox"/> No | <input checked="" type="checkbox"/> Other (specify): ADH IT |

If no, please provide a copy of the WIC State agency's ADP utilization plan.

- | | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

b. The State agency has written procedures for monitoring and approving local agency requests for ADP goods and services. If yes, please provide a copy of written procedures.

- | | |
|------------------------------|--|
| <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
|------------------------------|--|

ADDITIONAL DETAIL: Information System Appendix and/or Procedure Manual (cite):

2. System Documentation

a. The State system is fully documented in accordance with (check all that apply):

- | |
|--|
| <input checked="" type="checkbox"/> USDA/FNS Advanced Planning Document Handbook No. 901 |
| <input type="checkbox"/> USDA/FNS ADP Security Guide |
| <input checked="" type="checkbox"/> Other (specify): ADH IT Security Audit 2010 |

b. The State agency's overall ADP system documentation includes (check all that apply):

- | | |
|--|---|
| <input type="checkbox"/> a general design | <input checked="" type="checkbox"/> a detailed design |
| <input checked="" type="checkbox"/> user's manual | <input type="checkbox"/> maintenance manual |
| <input checked="" type="checkbox"/> method for updating documentation for system changes/modifications | |

Please provide copy of items checked off.

ADDITIONAL DETAIL: Information System Appendix and/or Procedure Manual (cite): Appendix I and II

III. INFORMATION SYSTEM (IS)

A. System Planning and Operation

3. Automated Data Processing Services

a. Indicate below whether the following ADP functions, if applicable, are performed by State agency/local agency staff or are contracted to an outside firm:

<u>Function</u>	<u>Performed SA/LA Staff</u>	<u>Contracted to Outside Firm (specify co. name):</u>
Data entry	<input type="checkbox"/> / <input checked="" type="checkbox"/>	_____
Food instrument production	<input type="checkbox"/> / <input checked="" type="checkbox"/>	_____
Management reports	<input checked="" type="checkbox"/> / <input checked="" type="checkbox"/>	_____
Feasibility study	<input type="checkbox"/> / <input type="checkbox"/>	_____
APD development	<input checked="" type="checkbox"/> / <input type="checkbox"/>	_____
ADP system hardware operation	<input checked="" type="checkbox"/> / <input type="checkbox"/>	_____
Custom software development	<input checked="" type="checkbox"/> / <input type="checkbox"/>	_____
Custom software maintenance	<input checked="" type="checkbox"/> / <input type="checkbox"/>	_____
Printing forms/FIs	<input type="checkbox"/> / <input checked="" type="checkbox"/>	_____
Backup computer facility	<input checked="" type="checkbox"/> / <input type="checkbox"/>	_____
Other (specify):		
<u>Software</u>	<input checked="" type="checkbox"/> / <input type="checkbox"/>	_____
Hardware	<input checked="" type="checkbox"/> / <input type="checkbox"/>	
	<input type="checkbox"/> / <input type="checkbox"/>	

b. The State agency has a blanket purchase agreement in effect (check all that apply): Please provide a copy of agreement. (See Appendix III)

equipment services software

c. The State agency has methods in place for ensuring that the cost of equipment or services used by WIC and other programs are equitably prorated among funding sources. Please provide policy of method used.

Yes No

The Arkansas WIC Program does not allocate the cost of equipment, as equipment is purchased solely for the use of the program, but we do allocate overhead services shared by the entire agency through indirect cost.

d. The State agency periodically reviews system costs billing

Yes No

e. The State agency acquires banking services through:

- competitive bids among banks within the State
- competitive bids among in-State and out-of-State banks
- use of State agency designated bank
- other:

III. INFORMATION SYSTEM (IS)

A. System Planning and Operation

f. The State agency acquires EBT services through:

- Competitive bids among EBT processors
- State agency IT services
- State hosted EBT services
- Other

ADDITIONAL DETAIL: Information System Appendix and/or Procedure Manual (cite): Appendix III

4. System Security/Data Confidentiality

a. To ensure that data files and computer programs are protected, the State agency ensures that (check all that apply):

- there is a separate organizational area/individual to control access to tapes, diskpacks or other electronic storage media.
- access to WIC Program data files is controlled through password access or similar control
- operational personnel are limited to only those jobs for which they are responsible
- passwords are protected
- passwords are changed periodically
- the system access procedures are audited at least once a year. Please provide a copy of access procedures. See Appendix I
- procedures are implemented for timely removing passwords, ID's etc. when personnel leave
- Biennial security reviews are performed by ADH IT Please provide a written summary of the most current Biennial security review. See Appendix IV, V
- Periodic risk assessments are performed by ADH IT
- Other (specify):

b. To ensure that disaster contingency plans (e.g., file storage, backup hardware, and software procedures) are sufficient to allow the management information and benefit delivery systems to recover and continue processing after fire, flood or similar disaster, the State agency ensures that (check all that apply):

- backup copies of files and program are stored off-site in a secure location. Please provide address of location
- backup copies are kept up-to-date
- there is an agreement with another processing unit with compatible hardware to provide services in an emergency. Please provide copy of agreement. See Appendix VI
- a contingency plan is in place in the event of service interruption. Please provide copy of contingency plan.
- a recent test of the WIC system or mock disaster recovery operation has been conducted at the backup facility. Please provide a written summary of the conducted test.
- other (specify): Right now, with DIS shifting the disaster recovery from Sunguard to DIS Data Center-West on April 1st things are still somewhat in flux. We still are

III. INFORMATION SYSTEM (IS)

A. System Planning and Operation

backing up all the WIC servers and data just as we have since Spirit came on line a few years ago so nothing has changed from the security and redundancy perspective. Once we have made the full switch over to DIS Data Center-West, we will be creating a new contingency plan and perform a test of the WIC system in disaster recovery operation. We will submit copies of both of these as an addendum, when they are completed.

**ADDITIONAL DETAIL: Information System Appendix
and/or Procedure Manual (cite): Appendix I, II, IV,V,VI**

III. INFORMATION SYSTEM (IS)

B. Participant Characteristics Supplemental Data Set

5. Description of IS changes that occurred in the past year:

<https://www.sugconnect.com/>

6. Description of IS changes planned for the upcoming year.

<http://www.wictechnologypartners.com/>; <https://www.sugconnect.com/>

Arkansas WIC will be making enhancements to the MIS that will include the ability to direct distribute special formula, and issue benefits using offline EBT. We have also made the proper changes to allow the MIS to issue a larger amount CVB to children, and issue CVB's to infants and pregnant women who are breastfeeding, in order to comply with the new food rule.

The Participant Characteristics (PC) Minimum Data Set (MDS) contains data items which are reported to FNS electronically by State agencies in April in even numbered years on all or a State-representative sample of participants. The MDS has required data items which must be collected and reported. The Supplemental Data Set (SDS) is comprised of data items which State agencies have agreed are desirable to collect and report at the national level. Please check MDS or SDS data items the State agency currently collects in its Information Systems and those MDS or SDS data items it is planning to collect within the next two years.

REQUIRED:

Participant Characteristics Minimum Data Set

State Agency IS Collects:

- State Agency ID.** A unique number that permits linkage to the WIC State agency where the participant was certified.
- Local Agency ID.** A unique number that permits linkage to the local agency where the participant was certified as eligible for WIC benefits.
- or**
- Service Site ID.** A unique number that permits linkage to the service site where certified. Either local agency ID or service site ID may be reported according to the level the State Agency feels appropriate. At a minimum, State agencies must provide agency names and addresses for each ID provided on their files.
- Case ID.** A unique record number for each participant which maintains individual privacy at the national level. (This may not be the case number used in the State agency's IS for the individual.) Participant or Case IDs for each participant should continue to maintain individual privacy at the national level.
- Client Date of Birth:** Month, day and year of participant's birth reported in MMDDYYYY format.
- Client Race/Ethnicity.** The classification of the participant into one of the five (5) racial/ethnic categories: For race: American Indian or Alaskan Native; Asian; Black or

III. INFORMATION SYSTEM (IS)

B. Participant Characteristics

Supplemental Data Set

African American; Native Hawaiian or Other Pacific Islander; and White. For ethnicity: Hispanic or Latino; Not Hispanic or Latino.

- Certification Category.** The category---one of five (5) possible categories---under which a person is certified as eligible for WIC benefits: pregnant woman; breastfeeding woman; postpartum woman (not breastfeeding); infant (under 12 months); or child (12-59 months).
- Expected Date of Delivery or Weeks Gestation.** For pregnant women, the projected date of delivery (MMDDYYYY format) or the number of weeks since the last menstrual period as determined at WIC Program certification.
- Date of Certification.** The date the person was declared eligible for the most current WIC Program certification. Month, day, and year should be reported in MMDDYYYY format.
- Sex.** For infants and children, male or female.
- Priority Level.** Participant priority level for WIC Program certification
- Participation in TANF, SNAP, Medicaid.** The participant's reported participation in each of these programs at the time of the most recent WIC Program certification
- Migrant Status.** Participant migrant status according to the federal WIC Program definition of a migrant farm worker (currently counted in the FNS 798 report).
- Number in Family/Household or Economic Unit.** The number of persons in the family/household or economic unit upon which WIC income eligibility was based. A self-declared number in the family/household or economic unit may be reported for participants whose income was not required to be determined as part of the WIC certification process. These participants include adjunctively income-eligible participants (due to TANF, SNAP, or Medicaid participation) and those participants deemed income eligible under optional procedures available to the State Agency in Federal WIC Regulations, Section 246.7(d)(2)(vi-viii) (means-tested programs identified by the State for automatic WIC Program income eligibility, income eligibility of Indian and in-stream migrant farmworker applicants).
- Family/Household or Economic Unit Income.** For persons for whom income is determined during the certification process, the income amount that was determined to qualify them for the WIC Program during the most recent certification. For descriptive purposes only, for participants whose income was not required to be determined as part of the WIC Program certification process, the self-reported income at the time of certification. These participants include adjunctively income-eligible participants and those persons deemed eligible under optional procedures available to the State Agency in Federal WIC Regulations, Section 246.7(d)(2)(vi-viii).

III. INFORMATION SYSTEM (IS)

B. Participant Characteristics

Supplemental Data Set

Zero should not be used to indicate income values that are missing or not available. Zero should indicate only an actual value of zero.

- Nutrition Risk(s) Present at Certification.** Up to 10 highest priority nutritional risks present at the WIC Program certification.
- Hemoglobin or Hematocrit.** That value for the measure of iron status that applies to the WIC Program certification. It is assumed that the measure was collected at the time of certification or within ninety (90) days of the certification date.
- Date of Blood Measurement.** The date of the blood measurement that was used during the most recent WIC Program certification in MMDDYYYY format.
- Weight.** The participant's weight measured according to the CDC nutrition surveillance program standards [nearest one-quarter (1/4) pound]. If weight is not collected in pounds and quarter pounds, weight may be reported in grams.
- Height.** The participant's height (or length) measured according to the CDC nutrition surveillance program standards [nearest one-eighth (1/8) inch]. If height is not collected in inches and 1/8 inches, height may be reported in centimeters.
- Date of Height and Weight Measure.** The date of the height and weight measures that were used during the most recent WIC Program certification in MMDDYYYY format.
- Currently Breastfed.** Information is needed for all infant participants ages six through thirteen months, whether or not the infant is currently receiving breastmilk.
- Ever Breastfed.** Information is needed for all infant participants ages six through thirteen months, whether or not the infant was ever breastfed.
- Length of Time Breastfed.** For infants ages six through thirteen months, the number of weeks the infant received breastmilk.
- Date Breastfeeding Data Collected.** For infants ages six through thirteen months, the date on which breastfeeding status was reported in MMDDYYYY format.
- Food Packages.** The food package code(s) for the WIC food package or for all food instruments prescribed for the participant during the month.

III. INFORMATION SYSTEM (IS)

B. Participant Characteristics Supplemental Data Set

OPTIONAL: Supplemental Data Set

State Agency IS:

Collects Plans to
 Collect

- Date of First WIC Certification:** Date the participant was first certified for the WIC Program in MMDDYYYY format. For pregnant, breastfeeding and postpartum women, this applies to the current/most recent pregnancy and not to prior pregnancies.
- Educational Level:** For pregnant, breastfeeding and postpartum women, the highest grade or year of school completed. For infants and children, the highest grade or year of school completed by mother or primary caretaker.
- Number in Family/Household on WIC:** The number of people in the participant's family/household receiving WIC benefits.
- Date Previous Pregnancy Ended:** For pregnant women, the date previous pregnancy ended in MMDDYYYY format.
- Total Number of Pregnancies:** For pregnant women, the total number of times the woman has been pregnant, including this pregnancy, all live births and any pregnancies resulting in miscarriage, abortion or stillbirth.
- Total Number of Live Births:** For pregnant women, the total number of babies born alive to this woman, including those who may have died shortly after birth.
- Pre-pregnancy Weight:** For pregnant women only, the participant's weight immediately prior to pregnancy. Pre-pregnancy weight may be reported either in pounds and ounces or in grams.
- Participant's Weight Gain During Pregnancy:** For breastfeeding and postpartum women, the participant's weight gain during pregnancy as taken immediately at or prior to delivery. Weight gain during pregnancy may be reported in either pounds and ounces or in grams.
- Birth Weight:** For infants and children, the participant's weight at birth measured according to the CDC nutrition surveillance program standards (lbs/ounces). Birth weight may be reported in either pounds or ounces, or in grams.
- Birth Length:** For infants and children, the participant's length measured according to the CDC nutrition surveillance program standards (1/8 inches). Birth length may be reported in either inches and eighth inches or in centimeters.

III. INFORMATION SYSTEM (IS)

B. Participant Characteristics

Supplemental Data Set

- Participation in the Food Distribution Program on Indian Reservations.**
The participant's reported participation in this program .

III. INFORMATION SYSTEM (IS)

C. WIC Systems Functional Requirements Checklist

The following checklists were taken from the WIC Functional Requirements Document (FRED) which is provided as guidance to State agencies on functions they should consider incorporating into their Information Systems. Please check those functions/capabilities which the State agency system currently performs or plans to perform within the next two years.

State Agency System Performs	State Agency System Planned	<u>Automated Core Function/Capabilities</u>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1. Calculates the date certification is due to expire.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	2. Assigns the participant a nutritional risk code and assigns a priority level. (CPA confirms the code is correct.)
<input type="checkbox"/>	<input type="checkbox"/>	2a. Assigns one risk code.
<input type="checkbox"/>	<input type="checkbox"/>	2b. Assigns up to 3 risk codes.
<input type="checkbox"/>	<input type="checkbox"/>	2c. Assigns up to 6 risk codes.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	2d. Assigns more than 6 risk codes.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	3. Calculates the applicant's household income and flags individuals whose income exceeds program standards.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	3a. Converts incremental income (weekly, monthly) to an annual figure.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	4. Associates family members.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	5. Statewide data is maintained to facilitate families transferring within the State.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	6. Transfers certification data to the central computer facility electronically either in real time or batch mode.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	7. Captures or documents the nutrition education provided each participant as well as the topics covered.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	8. Uses table-driven food packages.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	8a. Uses standard pre-defined food packages.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	8b. Enables easy food package tailoring.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	8c. Performs edits to prevent over-issuance during food package creation.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	9. Enables food instruments to be printed when the participant is present for pick-up, i.e., on-demand.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	10. Captures or documents the name of the programs to which the participant was referred.
<input type="checkbox"/>	<input type="checkbox"/>	11. Performs food instrument reconciliation.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	12. Produces standard Dual Participation Report.
<input type="checkbox"/>	<input type="checkbox"/>	13. Produces standard Integrity Profile (TIP) Report.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	14. Produces standard Rebate Billing Report.

III. INFORMATION SYSTEM (IS)

C. WIC Systems Functional Requirements Checklist

State Agency System Performs	State Agency System Planned	<u>Automated Core Function/Capabilities</u>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	15. Produces standard Participation Report.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	16. Produces Participant Characteristics Datasets.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	17. Captures basic transaction data by vendor.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	18. Flags high-risk vendors through peer group analysis of redemption data.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	18a. Identifies vendors with high average food instrument redemptions.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	18b. Identifies vendors with a narrow variation in redemptions.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	19. Assigns a maximum value for each food instrument type.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	19a. Checks redeemed price against maximum and rejects any food instruments exceeding the maximum amount.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	20. Captures source of income.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	21. Has the capability of annualizing household income occurring at more than one frequency.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	22. Performs automated dietary assessment.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	23. Has automated growth charts.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	24. Has point of certification data entry, i.e., a personal computer at each “station” within the clinic.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	25. Allows for ad hoc reporting.

ADH CENTRAL OFFICE SAFETY AND SECURITY PLAN

(See Memorandum No. 05-9, Subject: Electronic Protected Health Information, Date: February 23, 2005.)

Policy:

It is the policy of the Arkansas Department of Health to provide a safe and secure working environment for all employees.

The Arkansas Department of Health has an ADH Central Office Safety and Security Plan that covers emergency evacuation and relocation for the Central Office, which includes the Central Office and Public Health Laboratory. There is also a Freeway Medical Tower Safety and Security Plan for Arkansas Department of Health Employees. These Plans cover natural disasters, such as tornadoes, floods, earthquakes, fires, etc., and security incidents that could place employees or clients in potential danger.

If an employee in the Central Office, Public Health Laboratory, or Freeway Medical Tower will require assistance during an evacuation, the employee must complete an ADH Building Evacuation Assistance Request (AS-50) and submit to the appropriate Safety Officer. The Safety Officer:

- compiles a list of employees needing assistance and gives the list to the officer at the front Security Desk.
- updates the AS-50 if an employee relocates within the building or the request for assistance was temporary.
- transfers the AS-50 to the appropriate Safety Officer if the employee relocates, if applicable.

To access the ADH Central Office Safety and Security Plan, Freeway Medical Tower Safety and Security Plan for Arkansas Department of Health Employees, and a list of Safety Officers, go to the ADH Intranet Home Page.

ADH INFORMATION SYSTEMS PASSWORD REQUIREMENTS

I. Policies:

To access ADH information systems or application, users must authenticate identity by presenting acceptable credentials. Access privileges protected by user credentials can be compromised if the credentials are improperly stored or inadequately safeguarded.

See the Information Systems Security Access policy for related security requirements and a complete definition of terms.

This policy applies to ADH users, non-ADH users, and Systems Administrators in all ADH Centers/work units.

Definitions

ADH User: A person, ADH employee, who has been granted access to any ADH information system and is accountable for the security of such access.

Non-ADH User: A person, not an ADH employee, who has been granted access to any ADH information system and is accountable for the security of such access.

Access: Upon the presentation of authenticated credentials, permission to use ADH information systems.

Authentication: The automated comparison of presented user credentials with credentials on record for access to ADH information systems.

Credentials: Consists of the combination of a user's User Name (or similar user identifier) and password.

ADH Information Systems: ADH Network services (Network access, E-mail, Intranet, etc.), ADH applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the ADH devices for which it was intended. It also includes any computer file, on any device in use by ADH or its agents, that is shared across the ADH network or requires ADH support, or that contains ADH-related information, the privacy of which must be safeguarded.

System Administrator: Person designated by ADH's Chief Information Officer to provide technical support and access management for ADH information systems.

Person: One whose identity has been validated and whose association with ADH has been certified by the Center/work unit requesting access credentials.

Safeguarding of Credentials

Private or mission-critical information stored and processed on computer systems must be protected against unauthorized modification, disclosure, or destruction. Users are assigned a unique personal identifier which must be authenticated in conjunction with a valid password before access is granted to ADH information systems. Measures must be employed by users to safeguard credentials with respect to both physical security and access to ADH information systems. The structuring of passwords will meet or exceed prevailing state government standards for strong passwords.

Requirements

ADH information systems password construction will conform to the following standards. Password construction standards are also posted on the ADH Intranet under Office of Information Technology Systems.

A. Network Passwords

- a. Must be at least eight characters in length.
- b. Must contain at least one of each of the following: (a) Upper case alpha characters; (b) Lower case alpha characters; and (c) Numeric characters (1 through 9).
- c. May not be the same as any previous six passwords.

B. Password Selection: Users must make a good faith effort to select strong passwords composed of a collection of random characters, following construction rules outlined above, rather than weak passwords that may easily be guessed. Logical names and words, even in combination with a leading or trailing number, are weak passwords. Names spelled backwards, names of celebrities, well-known landmarks, popular culture icons, family names, etc., should be avoided in passwords.

C. Password Life Cycle: Passwords will expire in 60 days, or earlier if changed by the user. Users will receive system prompts, in advance of expiration, warning users to select a new password. Users may not reuse any of their last six passwords. A password should be changed if a user suspects its security has been compromised.

D. Physical Security: Sharing of credentials is strictly forbidden. Written recording of credentials is discouraged but, if recorded, the following rules should be observed:

- a. Never openly post user credentials, particularly in proximity to the user's PC.

- b. Store recording of credentials in a secure location.
- c. Do not identify the recording as a password.
- d. Do not include user name with password.
- e. Mix in false characters or scramble the password recording in a manner the user will remember so the written version is different from the real password.
- f. Never record a password on-line or include a password in an e-mail message.

E. Security of System Infrastructure

- a. Non-Technical Requirements: In order to maintain the security of ADH information systems, user access may be granted only after authentication through the presentation of acceptable credentials. Credentials are uniquely assigned to a person and may not be generically ascribed to groups or agents unless explicitly approved by ADH's Chief Information Officer.
- b. Technical Requirements: Technical requirements follow the Microsoft regimen.

Disciplinary Action for Violation of Policy

Supervisors should refer to the Employee Disciplinary Policy – Minimum Conduct and Performance, to determine the appropriate disciplinary action for violations of this policy.

II. Procedures:

- A. To Obtain User ID and Password for E-mail

Responsibility

Employee's Supervisor

Action

Contacts Center Personnel Coordinator to make request.
Note: Role-based access to specific data files or work unit application programs is assigned on an individual basis. (See Data Access policy to determine level.)

Responsibility

Action

Employee's Supervisor/
Personnel Coordinator

Prepares ADH Systems Security
Access Request (ADH-359) and
faxes to ITS Help Desk.

ITS Help Desk

Informs Personnel Coordinator of the
new ID and password within five
working days of receipt of the
request.

Personnel Coordinator

Informs employee of the new ID
password.

Employee

Changes password at least every 60
days.

B. To Alter or Delete User ID and Password

Responsibility

Action

Employee's Supervisor

Informs appropriate Personnel
Coordinator of employee's status
(moving or termination) immediately.

Employee's Supervisor/
Personnel Coordinator

Prepares ADH Systems Security
Access Request (ADH-359) and
faxes to ITS Help Desk.

ITS Help Desk

Denies access to specified user ID on
effective date.

ADH INTERNET FILTERING

Policies:

This policy defines the process for responding to requests for Internet filtering, for determining the types of Internet destinations that will be filtered, and for identifying its applicability to classes of ADH computer users.

This policy applies to all ADH Centers and all persons who use a computer attached to the ADH network.

See Information Systems Security Access for related security requirements and definitions of security terminology.

Definitions

Internet Filtering: The process of blocking or preventing access to Internet destinations.

ADMO: Associate Director for Management and Operations – ADH managers who have been authorized by each Center to certify user access requests. The role of the ADMO is to authorize the submission of security access requests for: (1) employees within the Center, and (2) non-ADH users affiliated with the Center. ADMO's are responsible for the validity of both ADH user and non-ADH user information in all User Access Account records they have authorized. See ADH Systems Security Access Request (ADH-359). ADMO's must notify the Gateway Administrator of material changes that affect both ADH user and non-ADH user access privileges. Only ADMO's will be recognized by the Security Gateway Administrator for the purpose of submitting user access requests.

Requirements

All requests for Internet filtering must be made to the ADH Chief Information Officer (CIO). Internet filtering is implemented by the Department of Information Systems (DIS).

Requests for Exemption

Individuals having devices that require access to blocked sites for ADH business-related purposes may request access for their specific use. Such requests must be approved by the employee's Center ADMO for consideration.

ADH REMOTE ACCESS POLICY

Policies:

This policy applies to all ADH information systems users in all ADH Centers/work units and to all non-ADH organizations to whom ADH offers remote access.

ADH users and non-ADH users, as defined in this policy, may use various forms of remote connection technologies to gain access to ADH information systems. Access requires the user to present authenticated credentials when prompted.

See the Information Systems Security Access policy for related security requirements and definitions of security terminology.

Definitions

Access: Upon the presentation of authenticated credentials, permission to use ADH information systems.

Credentials: A combination of a user's User Name (or similar user identifier), and Password. Users present credentials, when prompted, to access ADH information systems.

ADH Information Systems: ADH Network services (Network access, E-mail, Intranet, etc.), ADH applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the ADH devices for which it was intended. It also includes any computer file, on any device in use by ADH or its agents, that is shared across the ADH network or requires ADH support, or that contains ADH-related information for which the privacy is required to be safeguarded.

ADH User: An ADH employee who has been granted access to any ADH information system and is accountable for the security of such access.

Non-ADH User: A person, not an ADH employee, who has been granted access to any ADH information system and is accountable for the security of such access.

Remote Connection: Includes a variety of technologies that enable a user to connect to the ADH Network from devices not directly linked to ADH's Network. For ADH purposes, Virtual Private Network (VPN) technology is preferred. Methods typically in use include Terminal Server (TS), Remote Desktop Connection (RDC), and Remote Access Server (RAS). Typical hosting services enabling these methods include Internet Service Providers (ISP), connection through an organization's own internet hosting service, or dial-in through a telephone line (RAS).

Security Gateway Administrator: This function is housed at the ADH Help Desk. This role serves as the common point of entry for all user access requests. Primary functions include initial evaluation of received access requests, validation of identity, and re-directing of requests for additional processing.

Virtual Private Network (VPN): A VPN is a secure, private network that uses a public network (usually the Internet) to connect hosts (such as ADH's network) with remote users.

Request for Access

Requests for remote access must be submitted by the Center's Associate Director for Management and Operations (ADMO) to the Security Gateway Administrator using the ADH Systems Security Access Request (ADH-359). See the Information Systems Security Access policy for the ADMO's System Security Certification requirements.

ADMO's certify by signature on the ADH-359 the following:

- That such access requests are made on behalf of persons who are ADH employees in good standing, or if a non-ADH user, have been verified to be a member of an organization with whom a formal agreement is in place to permit access to ADH systems and to safeguard protected information.
- That users have provided accurate identifying information and that the user has a legitimate and official purpose for the requested level of access.
- That the users have been apprised of ADH policies pertaining to the appropriate use of state equipment and systems services, pertaining to the safeguarding of private information, and have received HIPAA privacy training as required by ADH policy or contracts.
- That they agree to notify the ADH Systems Security Gateway of material changes in users' employment status as relates to any ADH network services or systems applications for which users have been granted access.

Management of Authorizations

The Network Administrator maintains a list of users granted remote access privileges and submits a monthly report of such users to the ADH Information Systems Manager.

The ADH Chief Information Officer reserves the right to approve requests for remote access to ADH information systems and reserves the right to terminate access at any time.

Responsibilities of Remote Access Users

This policy applies to all ADH information systems users in all ADH Centers and to all non-ADH organizations to whom ADH offers remote access. It also includes persons who remotely access an ADH E-mail account, who remotely connect to an ADH application or network service, or who remotely connect to a computer device at their

work site. It applies without regard to: the remote connection method employed (see Remote Connection definition in this

policy); who pays for the method of connection; where the remote site is located; and what type of remote computer device is used.

Requests for remote access must be submitted using the ADH-359 through the user's Center ADMO. The ADH-359 requires the user's signature on a Security Agreement and Confidentiality Statement.

It is the responsibility of the user to comply with the ADH Information Systems Security Access policy and the terms of the signed Security Agreement and Confidentiality Statement.

It is the responsibility of remote access users to ensure that connection to ADH information systems is not used by unauthorized persons who may have access to their devices. Users must be made aware that remote access connects from their remote site (e.g., home, facility, travel locations, etc.) to the ADH Network, so that their device becomes an extension of the network and can provide a path to expose ADH's most sensitive information. The user must take every reasonable measure to protect ADH information systems from intrusion and exposure.

Disciplinary Action for Violation of Policy

Supervisors should refer to the Employee Disciplinary Policy – Minimum Conduct and Performance to determine the appropriate disciplinary action for violations of this policy.

AFTER HOURS ENTRY - CENTRAL OFFICE

I. Policies:

All entrances are locked before 6:30 a.m. and after 5:00 p.m. on regular work days.

Department of Health employees who enter and exit the building before/after business hours on weekdays or on holidays must have a current ID/access badge with a minimum 24/7 security level. Employee's security levels are based on the ID Card Request for Central Office and Freeway (AS-39) and the ADH Systems Security Access Request (ADH-359).

Visitors, workmen and others who enter and exit the building before/after business hours, on weekends, and on holidays must be accompanied by an ADH employee with a minimum 24/7 security level. The ADH employee is responsible for the visitor signing in/out.

Disciplinary policies for gross negligence apply to any employee who exits the building after hours by unlocking doors or removing the orange security bar from any door.

II. Procedures:

A. Employees entering and exiting the building

1. Enter through the Southwest (front) door, Southeast (rear) door, or Director's Door (Annex).
2. Place ID/access badge on card reader to enter or exit building.

B. Persons (non-employees) attending meetings in the building after hours

1. The person in charge must:
 - Notify the Physical Plant Section Chief or Building and Supply Services Leader for the meeting to be held after hours. (See Meeting Rooms/Videoconferencing/Satellite Downlink Stations policy in this Volume.)
 - Provide a sign-in sheet to record participants' names.
 - At the meeting time, enter building at the west basement door. State name and reason for entry and sign-in.

- Provide to operator a list of meeting participants' names so they can be admitted upon arrival for the meeting.

- Have meeting participants sign in on sheet obtained from operator and stay in the meeting area, which includes meeting room, nearby hallways and restrooms.
- When the meeting is over, return the completed sign-in sheet to the Security Guard desk. Participants are escorted by the “person in charge” to one of three 24/7 exit doors or the west basement door. The “person in charge” uses his ID/access badge to open for participants to exit.
- Sign out and exit.

| C. Persons (non-employees) such as repairmen, plumbers, pest-control technicians, etc. entering the building.

1. Inform the Physical Plant Section Chief ahead of time when they will be working.
2. Enter building through southeast (rear) door. Provide name, identification and reason for entry. Complete sign-in log information.
3. After work is finished, return to Physical Plant area. Complete sign-out log information.
4. Exit building through southeast (rear) door.

CONFIDENTIALITY/BUSINESS ASSOCIATE AGREEMENTS/
CONFIDENTIALITY CONTRACT PROVISION

Policies:

Volunteer/Student/Extra Help Employee Confidentiality Agreement

Volunteers, students, extra help employees, and other individuals, such as school nurses or interpreters, in the LHU's and other work sites may be exposed to private information that is written, spoken or observed.

Private information may be information that belongs to a client, employee, or other volunteer or student. All private information must remain confidential and be maintained in a confidential manner.

Volunteers, students, extra help employees, and other individuals, such as school nurses or interpreters, are informed of their obligations regarding management of private information, including the HIPAA privacy policies that pertain to their activities at ADH, during orientation. Understanding and agreement are documented using the Confidentiality Agreement (AS-32) before they are allowed to observe in or perform duties for the Agency.

Note: Volunteers must be aged 18 years or older.

Business Associate Agreements

ADH enters into Business Associate Agreements with applicable entities if 1) services provided involve disclosure of PHI, AND 2) functions or activities are performed on behalf of ADH, e.g., shredding company, software vendor. (See Business Associate Agreements policy in the HIPAA section of this Volume.)

Send any requests for Business Associate Agreements to the ADH Privacy Officer.

Confidentiality Contract Provision

Add the following addendum to any contracts that involve disclosure of PHI, e.g., letter of appointments. Contact the ADH Privacy Officer or Agency Legal Team with any questions.

Addendum: You agree to maintain and disclose any Protected Health Information (PHI), as defined in the federal regulations, in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Standards (U.S.C. 1320d et seq.) and its implementing regulations including, but not limited to, 45 Code of Federal Regulations (CFR) parts 142, 160, 162 and 164 and hereinafter referred to as the Privacy Rule. You must further comply with any other applicable federal law and regulation. You further

agree to maintain the confidentiality of PHI and not exceed the limitations applicable under the HIPAA regulations.

DATA ACCESS

I. Policies:

Access to data by ADH employees is granted at increasingly responsible levels based on the following System Criticality chart:

	LEVEL 1 – NOT CRITICAL Necessary to state government but short-term interruption of service acceptable. These systems do not play any role in the scheme of health, security, safety of the citizens, etc. They could be easily offset with manual procedures.	LEVEL 2 – CRITICAL Required to perform a critical service of state government. These systems will be required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the system can be restored.	LEVEL 3 – EXTREMELY CRITICAL Critical to health or safety. These systems must be protected by a vital plan that would ensure resumption of operations within a very short timeframe.
LEVEL A – UNRESTRICTED Open public data with no distribution limitations, anonymous access. May be anonymous access via electronic sources. Examples: Arkansas.gov website, ADEQ website, and other state agency public websites	1A	2A	3A
LEVEL B – SENSITIVE Public data with limited availability, but which requires a special application to be completed or special processing to be done prior to access (for example, to redact sensitive data elements). Examples: Most data elements in the state personnel records, data elements in motor vehicle records not restricted by privacy regulations, and driver history records	1B Central Drug and Supply Meeting Room Agency Carpool Franchise Numbers	2B	3B
LEVEL C – VERY SENSITIVE Data only available to internal authorized users. May be protected by federal and state regulations. Intended for use only by individuals who require the information in the course of performing job functions. Examples: Social Security numbers, credit card numbers, home addresses, and competitive bids	1C	2C EPIT	3C Search Patient Scheduler Search Org Role Search
LEVEL D – EXTREMELY SENSITIVE Data whose disclosure or corruption could be hazardous to life or health. Examples: Contents of state law enforcement investigative records and communications systems	1D	2D	3D TB Mgmt System User Profile Role Map IT Leaders HELP Desk TPR – Billing EHD – Infant NBS IHS

SENSITIVITY LEVELS

Level A – Unrestricted

Unrestricted data is characterized as being open public data with no distribution limitations and to which anonymous access is allowed.

These data elements form information that is actively made publicly available by state government. It is published and distributed freely, without restriction. It is available in the form of physical documents such as brochures, formal statements, press releases, reports that are made freely available, and in electronic form such as internet web pages and bulletin boards accessible with anonymous access.

The greatest security threat to this data is from unauthorized or unintentional alteration, distortion, or destruction of this data. Security efforts appropriate to the criticality of the system containing this data must be taken to maintain its integrity.

Examples of data at this sensitivity level include many agency public websites.

Level B – Sensitive

These data elements are the information that is made available through open records requests or other formal or legal processes. This category includes the majority of the data contained within the state government electronic databases. Direct access to this data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties.

Security threats to this data include unauthorized access, alteration and destruction concerns.

Examples:

Most data elements in state	Building code violations data
personnel records	Collective bargaining data
Driver history records	Federal contracts data
Employment and training	Historical records repository
program data	data
Firearm permits data	Occupational licensing data
Medical examiner and coroner data	Real estate appraisal data
Personnel data	

Level C – Very Sensitive

Data classified as being very sensitive is only available to internal authorized users and may be protected by federal and state regulations.

Very sensitive data is intended for use only by individuals who require the information in the course of performing job functions.

These data elements include those protected by federal and state statute or regulation. Access to these data elements is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties. These are the data elements removed from responses to information requests for reasons of privacy.

Security threats to this data include violation of privacy statutes and regulations in addition to unauthorized alteration or destruction. If this data were accessed by unauthorized persons, it could cause financial loss or allow identity theft. Unauthorized disclosure could provide significant gain to a vendor's competitors.

Examples:

Social Security numbers	Credit card numbers
Most home addresses	Competitive bids
Attorneys' files	Civil investigative data
Comprehensive law enforcement data	Criminal history data
Domestic abuse data	Economic development assistance data
Educational records	Food assistance programs data
Foster care data	Head Start data
Health and medical data	Juvenile delinquent data
Library borrower's records	Counselors' data
Signature imaging data	Trade secrets data
Welfare records/data	

Level D – Extremely Sensitive

Data classified as being extremely sensitive is data whose disclosure or corruption could be hazardous to life or health.

These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health or safety repercussions. Very strict rules must be adhered to in the usage of this data.

Examples of this data include the contents of state law enforcement investigative records and communications systems.

CRITICALITY LEVELS

Level 1 – Not Critical

These data and systems are necessary to state government but short-term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of Arkansas' citizens.

Level 2 – Critical

These data and systems are required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the data and systems can be restored.

Level 3 – Extremely Critical

These data and systems are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe.

Access to data by employees is role-based. All employees are subjected to an appropriate level of security clearance before they are hired, transferred or promoted.

Job descriptions must indicate on a broad level the expected access of the data the employee will analyze and the data the employee will generally use. Job-related "need to know" is used as the basis for determining database access by a given employee.

In conjunction with appropriate technical support staff, the custodians of the data, and the employee, the supervisor determines the level of access based on the need for access to perform job duties.

Data Access Review

Role-based access must be reviewed by the employee's supervisor for accuracy at least every six months. A copy of the report must be submitted to the ADH Privacy/Security Officer by February 1 and August 1 each year. Note: IS Leaders have the capability to print reports.

E-MAIL USAGE POLICY

Policies:

The purpose of this policy is to define the terms and conditions under which the Arkansas Department of Health (ADH) e-mail system may be used. It applies to any user of ADH information systems. The ADH Chief Information Officer, Office of Information Technology Services, manages access to ADH information systems, including e-mail.

E-mail access is provided as a service to ADH employees and affiliates for the purpose of supporting the Department's mission. Access is used in a manner that maintains public trust and confidence.

Definitions

Access – Upon the presentation of appropriate credentials (user name and password), permission to use ADH information systems, including the e-mail system, is granted according to requirements set forth in the Information Systems Security Access policy.

ADH Information Systems – ADH network service (network access, e-mail, Internet, etc.), ADH applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the ADH devices for which it was intended.

User or End User – A person who has been granted access to any ADH information system. A user may be an ADH employee or an employee of an ADH affiliate.

Public Record – As defined in Ark. Code Ann. §25-19-101, a public record may exist in “any medium” and “all records maintained in public offices or by public employees within the scope of their employment shall be presumed to be public records.”

E-mail System – Description and Terminology

E-mail consists of an evolving and growing range of network based messaging, calendaring, contact, and other on-line information management services. An e-mail system is deployed by an e-mail provider through an infrastructure of network devices consisting primarily of e-mail services and e-mail clients on end user PCs.

E-mail Provider – An agent who deploys and manages an e-mail system.

E-mail Server – Equipment and software (e.g., Microsoft Exchange) dedicated to providing an e-mail system for a population of network user.

E-mail Client – The PC and software (e.g., Microsoft Outlook) used by an end user for the purpose of accessing an e-mail system.

E-mail Address – The address used by an e-mail server to route messages to addressees (e.g., John Doe or John.Doe@mymail.com).

E-mail Record – Recorded user interaction or transaction history associated with any aspect of the ADH e-mail system is an e-mail record. E-mail records are public records subject to rules of privacy, disclosure and retention. Examples of e-mail records include e-mail messages, calendars, contacts, ADH e-mail addresses.

ADH E-mail Account – Approved users reassigned a unique e-mail account that enables validation of user identity and authentication of access requests. The ADH e-mail account is a unique identifier that associates a user with e-mail activity stored on the e-mail server. Users are responsible for the security of their e-mail account as specified in the ADH Systems Security Access Request (ADH-359) and the Information Systems Security Access policy.

E-mail Mailbox – User activity is displayed on the e-mail client in a virtual mailbox. The mailbox is a visual representation of the types of services offered by an e-mail client. These typically include Inbox, Sent Items, Deleted Items, Calendar, Contacts, etc. Users are responsible for managing their own mailbox within limitations provided for overall account space and size of individual messages.

E-mail Authoring – Authoring includes drafting, sending, replying or forwarding an e-mail message. See rules pertaining to responsibility for authorship in this policy.

E-mail Possession – A user is in possession of an e-mail message when the e-mail server delivers it to the user's e-mail client. See rules pertaining to responsibility for possession.

E-mail Client Features – For the purpose of determining responsibility for authorship or possession of any given message, the content and transaction of the following typical e-mail client features should be evaluated: Message Authoring; Message Received; Message Reply; Message Forward; Sent Message; Message Read, Opened or Previewed, Message Headers; Message Internet Headers Message Body, Personal Folders (a term used by Microsoft Outlook to identify file space on a local PC where mailbox items can be stored).

E-mail Signature – Allowed information includes an employee's name, title, work address and telephone, fax telephone and e-mail address. Personal tag lines and icons are not allowed in e-mail signatures.

General Provisions

The ADH e-mail system and all associated e-mail records, ADH e-mail addresses, and ADH e-mail accounts and mailboxes are the property of the State of Arkansas.

ADH reserves the right to monitor and log all network activity with or without notice, including e-mail and all web site communications. Users have no reasonable expectation of privacy in the use of these resources. All violations are subject to disciplinary action as outlined in the Employee Disciplinary Policy – Minimum Conduct and Performance.

Allowable Use: E-mail is provided to employees and affiliates for the purpose of supporting the Department's mission. Use of e-mail is encouraged to:

- A. Enhance the conduct of ADH business by facilitating the exchange of information within ADH, with other state and federal agencies, with ADH business partners, and with the public.
- B. Provide rapid and comprehensive access to data sources to assist employees in fulfilling their ADH responsibilities.
- C. Facilitate in the performance of required ADH tasks or projects.
- D. Communicate information related to professional development or to maintain currency on topics of public health interest.
- E. Encourage collaborative projects and sharing of resources.
- F. Receive announcements of new laws, rules or regulations.

E-mail may be occasionally used for personal purposes provided that it does not interfere with ADH information systems or the ADH e-mail system, burden the Agency with added administrative or incremental system costs, or interfere with the user's employment responsibilities.

Restrictions: E-mail may not be used for:

- G. Sending, receiving, printing or otherwise disseminating proprietary data or other confidential or sensitive information of the Arkansas Department of Health in violation of Department, State, or Federal policy or proprietary agreements.
- H. Viewing, downloading or sending pornographic or other obscene materials.
- I. Visiting and/or participating in chat rooms not designated for professional interactions specifically related to one's job.
- J. Disseminating or printing copyrighted materials (including articles and software) in violation of copyright laws.
- K. Intentionally disrupting network or system use by others, either by introducing worms, viruses, virus hoaxes or by other means.
- L. Commercial or fund-raising purposes not under the auspices of ADH.
- M. Operating or promoting a business or soliciting for personal gain.
- N. Promoting any political campaign.

- O. Using offensive or harassing statements or language maliciously disparaging others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs. An exception would apply when such language or statements are included as objective citations in the conduct of official ADH business.
- P. Without proper authorization, seeking information from another user's PC, copying or modifying another user's files or data, or using passwords belonging to another user.
- Q. Sending e-mail messages under the following conditions: anonymous authoring, employing a false identity, misrepresenting oneself as a state agency, as the Legislature, as a legislator, falsely representing oneself as a state employee or as an agent of the state (including unauthorized use of another's password or log-in code).
- R. Interfering or causing excessive load on ADH information systems or the disrupting of others' use of the e-mail system. Such uses include, but are not limited to, sending or forwarding of chain letters, Spam, hoaxes, mass mailings not related to ADH business, introducing worms, viruses or messages containing malicious code.
- S. Transmitting or, with foreknowledge, receiving offensive or sexually oriented material.
- T. Engaging in any activity in violation of minimum standards of conduct as defined in the Employee Disciplinary Policy – Minimum Conduct and Performance.

Service Restrictions

- A. Users are expected to use ADH information systems responsibly, to comply with laws, policies, and regulations governing the use of e-mail, and to exercise professional and personal courtesy in the use of both.
- B. Access to the ADH information systems is a privilege that may be wholly or partially restricted without prior notice.
- C. Users may hold to no expectation of privacy in the use of ADH information systems.
- D. ADH reserves the right to monitor all aspects of e-mail usage.

Misuse

- 1. Evidence of misuse may result in termination of access to ADH information systems without prior notice. Theft or abuse of ADH information systems, including the e-mail system, is subject to penalties imposed by law and ADH policies.

2. Misuse includes, but is not limited to:
 - A. Theft, unauthorized disclosure, unauthorized destruction of e-mail records
 - B. Unauthorized entry, use, transfer, and tampering with one's own e-mail account or the accounts and e-mail records of others
 - C. Interference with others' work in the use of ADH information systems
 - D. Failure to comply with rules of privacy and disclosure
 - E. Failure to comply with the rules of allowable use

Disclaimers

ADH cannot protect users from receiving e-mail they may find offensive. ADH cannot guarantee protection from e-mail messages containing viruses, worms, malicious attachments or malicious code. ADH cannot guarantee that any received message was in fact sent by the purported sender. ADH cannot assure that original content in any forwarded message, or message replied to, had not been modified.

Responsibility for Authorship or Possession of E-mail

Responsibility: A user may be held accountable for authorship or for possession of an e-mail message. Responsibility applies to two types of messages: those authored by the user and those received by the user.

Responsibility for Messages Authored: A user assumes authorship responsibility for: (1) the content of any e-mail message authored by the user, and (2) for user authored revisions in messages replied to or forwarded. A user assumes no authorship responsibility for messages sent by a third party, in the user's name, and without the user's knowledge.

Responsibility for Messages Received

- When the e-mail server deliver an e-mail message to the user's mailbox, the user is considered to be in possession of the received message, but is held accountable only for those portions of the received message that may have been authored or revised by the user.
- An e-mail user assumes responsibility for possession of messages delivered to user's mailbox under the following circumstances:
 1. When the user effectively exercises control of authorship of a received message. Control of authorship includes but is not limited to forwarding or replying to a received message (whether or not the original message is modified);

2. When the user exercises control over the storage of a received message, received messages deleted from a user's mailbox, and not stored, are not considered to be the user's responsibility if such messages were not authored by the user;
3. Exercising control of the storage of a message includes, but is not limited to: saving the message anywhere on the e-mail server, saving the message to any medium off the e-mail server (e.g., CD, hard drive, storage device, server share, etc.), moving the message to Personal Folders.

Security and Confidentiality of E-mail

E-mail records are subject to the same rules, with respect to employee responsibilities for safeguarding privacy and preventing unauthorized disclosure, as ADH records created in any other communication medium.

E-mail records are subject to ADH policies and statutes pertaining to HIPAA. Users are subject to penalties for violation of HIPAA rules and for violations of related Arkansas laws and ADH policies.

Confidentiality of e-mail cannot be assured. E-mail security should always be assumed to be reactive rather than preventive of potential malicious intrusions. Extreme caution should be exercised in using e-mail for confidential or sensitive matters.

E-mail's ease of distribution and its unrestricted copying and forwarding features make its use highly susceptible to breaches of confidentiality. E-mail intended for one person may be widely forwarded to others, may be posted to bulletin boards or subscription services, may be attached for other messages, may be saved in other users' mailboxes, and may persist in system backups and archives.

E-mail records are subject to disclosure in response to Freedom of Information Act requests, subpoenas for legal and administrative hearings, and client requests for access to pertinent case records. Before releasing information in such cases, related ADH policies should be consulted and guidance obtained from Legal Services.

Archiving and Retention of E-mail

Arkansas law pertaining to records retention does not distinguish between media with regard to the definition of Public Record. E-mail records are subject to the provisions of Arkansas records and retention statutes and subject to retention requirements specified in regulations governing conduct of programs administered by ADH.

Disciplinary Action for Violation of Policy

ADH employees are subject to disciplinary action for violations of this policy as provided in the Employee Disciplinary Policy – Minimum Conduct and Performance.

IDENTIFICATION/SECURITY ACCESS CARDS

I. Policies:

The Department of Health requires every employee to obtain and wear an Identification Card (ID) while on duty so that it is always visible, face front. Extra help, part-time, and interns also must obtain and wear an ID Card. New employees are required to obtain an ID Card within 10 working days of employment. Employees on the Markham Street campus are also required to have a Security Access Card. ID Cards must be renewed every one to three years, depending on their access designation. Upon card expiration, termination, resignation, or retirement, the employee must return the ID Card and Security Access Card, if applicable, to his/her immediate supervisor.

Each employee is given a building security access designation.

- A. Access to the Emergency Operations Center (EOC) must be authorized by the Preparedness and Response Director or designee.
- B. Access to the Secured Communications Center (SCC) must be authorized by the Department of Health Director or designee.
- C. Access to Public Health Laboratory (PHL) areas (location, level, and time) must be authorized by the Laboratory Director per the PHL's internal laboratory security plan. Additionally, permission for visitor's access and the access level (escorted/unescorted) to the PHL must also adhere to the PHL's internal security plan.
- D. Access level of an employee may be reviewed at any time by management.
- E. Security Access Cards are issued to employees who are stationed in the Markham Street Office. Employees stationed in other locations are issued Security Access Cards on a case-by-case basis.

Identification Card Security Access Code Definitions

Markham Street Main Office Security Access Cards

Color	Access Designation	Description	Expiration
None	Normal Day	Access to unsecured areas of building from 6:00 AM until 6:00 PM Monday thru Friday	3 years
Purple	Extended	Access to unsecured areas of building from 6:00 AM until 11:00 PM Monday thru Friday	3 years

Markham Street Main Office Security Access Cards (cont.)

Color	Access Designation	Description	Expiration
Green	24-Hour	Access to unsecured areas of building during all hours, including weekends	3 years*
Blue	Emergency Operations Center (EOC)	Access to unsecured areas of building during all hours, including weekends; also access to Emergency Operations Center	1 year
Red	Secured Communications Center	Access to all areas of building during all hours, including weekends; access to Emergency Operations Center; access to Secured Communications Center	1 year

Public Health Laboratory Security Access Cards

Color	Access Designation	Description	Expiration
None	Unsecured Areas Only	Access to unsecured areas of Public Health Laboratory	3 years
Green	Administrative Areas	Access to administrative areas	3 years
Red	All Areas	Access to all administrative areas and laboratories except the Select Agents Laboratory	1 year
Yellow	Select Agents	Access to all administrative areas and laboratories; unescorted access to areas storing and analyzing Select Agents. (Must have Department of Justice clearance for Select Agents.)	1 year

Lost or stolen ID and/or Security Access Cards must be reported to Human Resources or the Regional Director/designee within one working day. Lost or stolen Security Access Cards for the Public Health Laboratory must also be reported within one working day to the Public Health Laboratory Director or his designee.

An employee is given five days to locate a lost Security Access Card before a new card is issued. Lost or stolen ID Cards must be reported to Human Resources for Central Office employees or to the Regional Director or designee for field employees.

If an employee has lost three Security Access Cards within a two year time period, appropriate disciplinary action regarding lost property must be taken by his/her supervisor. If an employee receives a Security Access Card that does not work correctly through no fault of the employee, the card is replaced and the replacement is not counted against the employee as a lost card.

*ID and Security Access Cards may be requested for non-ADH personnel and are issued for one year only.

II. Procedures:

- Issuing New Cards, Updating or Changing Security Access, Replacing Lost or Expired Cards

- Central Office

Responsibility

Action

Immediate Supervisor

Completes and submits ID Card Request for Central Office and Freeway (AS-39) to Center(s) for signature(s).

Center Assistant Director for Management and Operations

Approves access designation(s) and obtains additional approvals, if necessary.

Center Personnel Coordinator

Completes AS-39. Obtains signatures. Files AS-39.

Sends electronic request to ADH Help Desk.

ADH Help Desk

Enters information into security database.

Human Resources

Takes photograph, prepares ID Card, and issues ID Card to employee.

Employee

If applicable, turns in expired ID Card to Human Resources.

Human Resources

If applicable, destroys old ID Card. Notifies Building Supply Manager of any change involving Security Access Card.

2. Field

Responsibility

Action

Immediate Supervisor

Completes and submits ID Card Request for Field (AS-40) to Regional Director for approval.

Regional Director/Designee

Approves access designation(s) and obtains additional Center approvals, if applicable.

Responsibility

Action

Regional Personnel
Coordinator

Verifies signatures and security levels on
AS-40.

Sends electronic request to ADH Help Desk.

ADH Help Desk

Enters information into security database.

Employee

Has photograph taken at designated
location. Note: Photographer ensures that
all pictures are 1024 dpi,
have a white background,
are a head and shoulder
shot, and are approved by
the employee.

Regional Personnel
Coordinator

Prepares ID Card and issues the ID Card
to the employee.

Note: A supply of ID Cards has been
issued to each Regional Office.

Employee

If applicable, turns in expired ID Card to
Regional Personnel Coordinator.

Regional Personnel
Coordinator

If applicable, destroys old ID Card.
Notifies Building Supply Manager of any
change involving Security Access Card.

3. ID Card Renewal

Responsibility

Action

ADH Help Desk

Sends notification of upcoming
expiration to employee and Personnel
Coordinator.

Employee

Updates information on AS-39 or
AS-40 and submits through
appropriate approvals to Personnel
Coordinator.

Personnel Coordinator

Verifies signatures and security levels.
May take updated picture of employee.

| Requesting Security Access Card for Employee Not Stationed in Markham
Street Building

Responsibility

Action

Immediate Supervisor

Sends request for Security Access Card to Regional Director or Center ADMO with justification.

Regional Director or

If approved, sends request for Center ADMO Security Access Card to Building Supply Manager.

Building Supply Manager

Notifies ADH Human Resources of approval to issue Security Access Card.

| Employee

Picks up Security Access Card from ADH Human Resources.

| C. Collecting ID Card from Terminated Employee (Central Office and Field)

Responsibility

Action

| Immediate Supervisor

Collects ID Card from employee on the date of termination. Notifies Human Resources immediately to deactivate the card. Includes ID Card with termination documents.

| Human Resources

Notifies Building Supply Manager of any change involving Security Access Card.

INFORMATION SYSTEMS SECURITY ACCESS

Policies:

Access to ADH information systems is managed by the ADH Chief Information Officer (CIO), Office of Information Technology Services, by means of an integrated systems security gateway. This policy applies to all ADH Centers.

All persons requiring access to ADH information systems must obtain permission from their Center's Associate Director for Management and Operation (ADMO) and must be authenticated through the CIO's designated Systems Administrators. All users must access ADH information systems through the Integrated Systems Security Gateway. ADH network services (including but not limited to E-mail and Internet), mainframe services, all major ADH applications, all Center-managed applications and Center files shared across the network must be accessed through the presentation and authentication of network credentials. Access to the Internet through the ADH network, without network authentication, is prohibited.

Definitions

Access: Upon the presentation of authenticated credentials, permission to use ADH information systems.

ADH Systems Security Access Request: The ADH-359, which is submitted to gain access to ADH network and application services.

Authentication: The automated comparison of presented user credentials with credentials on record for access to ADH information systems.

ADH Information Systems: ADH Network services (Network access, E-mail, Internet, etc.), ADH applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the ADH devices for which it was intended. It also includes any computer file, on any device in use by ADH or its agents, that is shared across the ADH network or requires ADH support or that contains ADH-related information, the privacy of which must be safeguarded.

Person: Someone whose identity has been validated and whose association with ADH has been certified by the Center requesting access credentials. A person may or may not be an ADH employee.

Integrated Systems Security Gateway: Common point of entry for all security access requests and authorizations.

User Access Account: A record, specific to a person and maintained by ADH Network Administrators, containing a user's identifying information and recording types and history of user permissions to ADH information systems. User access accounts must be attributable to an accountable person.

Generic Access Account: Systems access permissions based on a user name attributable to a system or business process. Such accounts may exist only on an exception basis, require CIO approval, and must be attributable to an accountable person.

Credentials: Consists at a minimum of the combination of a user's User Name (or similar user identifier) and Password. Users present credentials, when prompted, to access ADH information systems.

Validation of Identity: The process of substantiating that users are who they purport to be. User demographic and personnel identification information is received by the Security Gateway Administrator, is compared against validation data sources, and is re-confirmed by challenge-response contact with user.

Systems Security Roles

User: A person whose identity has been validated, whose association with ADH has been certified by the Center with whom the person is affiliated, who has been granted access to any ADH information system, and who is held accountable for the security of such access. A user may or may not be an ADH employee.

ADH User: A person, ADH employee, who has been granted access to any ADH information system and is accountable for the security of such access.

Non-ADH User: A person, not an ADH employee, who has been granted access to any ADH information system and is accountable for the security of such access.

System Administrator: For the purpose of this policy, this term collectively refers to persons exercising the following systems security roles: Security Gateway Administrator, Network Services Administrator, Mainframe Services Administrator, Windows Application Security Administrator, Mainframe Application Security Administrator, Systems Administrators for Center-supported applications, ADH Chief Information Officer. The role of such persons is to provide technical support and access management for ADH network services and applications.

Security Gateway Administrator: Persons located at the ADH Help Desk performing this role serve as the common point of entry for all user access requests. Primary functions include initial evaluation of received access requests, validation of identity, and re-directing of requests for additional processing.

ADMO: Associate Director for Management and Operation – a class of ADH managers who have been authorized to certify user access requests. The role of the ADMO is to authorize the submission of the ADH System Security Access Requests (ADH-359) for (1) employees within the Center, and (2) non-ADH users affiliated with the Center. ADMO's are responsible for the validity of both ADH user and non-ADH user information in all User Access Account records they have authorized. ADMO's must notify the Gateway Administrator of material changes that affect both ADH user and non-ADH user access privileges. Only ADMO's are recognized by the Security Gateway Administrator for the purpose of submitting user access requests.

System Security Certification

ADMO CERTIFICATION: Authorized ADMO's certify by signature on the ADH-359 the following:

- A. That such access requests are made on behalf of persons who are ADH employees in good standing, or if a non-ADH user has been verified to be a member of an organization with whom a formal agreement is in place to permit access to ADH systems and to safeguard protected information;
- B. That users have provided accurate identifying information and have a legitimate and official purpose for the requested level of access;
- C. That the users have been apprised of ADH policies pertaining to the appropriate use of state equipment and systems services, pertaining to the safeguarding of private information, and have received required HIPAA (Health Information Portability and Accountability Act) privacy training;
- D. The ADMO agrees to notify the Security Gateway Administrator of material changes in users' employment status as it relates to the ADH network services or systems applications to which users have been granted access.

USER SECURITY AGREEMENT AND CONFIDENTIALITY STATEMENT: Users certify by signature on the ADH-359 the following:

- That the user understands access to state-furnished equipment, software, and data is restricted to authorized persons only and may be used for official business purposes only;
- That the user accepts responsibility for appropriate use of state-furnished equipment and understands that computer devices, network activity, e-mail, and Internet access may be monitored to detect improper or illicit activity;
- That the user understands he/she may hold to no expectation of privacy in the use of state-furnished computer equipment and services;
- That the user understands system credentials allow access to all ADH network services, associated data, and system applications; the user agrees to take all necessary measures to safeguard the security of his/her access credentials; the user agrees not to share passwords nor employ them in a manner that compromises their security; the user understands he/she will be held accountable for any unauthorized usage of access credentials that results from his/her negligence or purposeful action; the user agrees to immediately report to Office of Information Technology Services any compromise of access credentials;

- That the user understands it is a violation of state and federal law to use, or permit the use, or fail to safeguard the security of client information in any way that jeopardizes its confidentiality;
- That the user understands he/she is subject to ADH policies pertaining to safeguarding of private information, penalties for inappropriate use of state equipment and electronic communication services, and sanctions for violations of related ADH Conduct Standards;
- That the user understands penalties for unauthorized access or inappropriate usage, for ADH or non-ADH users, may include discipline and/or prosecution.

Integrated Systems Security Gateway

ADMO's must certify each person as requiring and eligible for access to ADH network and application services using the ADH-359. The ADH-359 will be completed and faxed to the Security Gateway Administrator.

The ADH-359 collects demographic information necessary to establish user identity, physical location, window of usage, type of access and services required, all in sufficient detail to satisfy basic security and audit requirements. The form provides detailed user instructions concerning appropriate usage and ADMO certification language. The form requires user signature and ADMO signature.

The initial basis for establishing user identity for ADH users is the user's and the ADMO's AASIS Personnel Number. For non-ADH users, the initial basis is the user's SSN and the ADMO's AASIS Personnel Number. For ADH users not yet assigned an AASIS Personnel Number, identity may be provisionally established for 21 days by providing user's SSN. There is no provisional access for non-ADH users.

Upon receipt of the ADH-359, the Security Gateway Administrator will match identity data against validation data sources.

If a match exists for ADH users, the user will be contacted by telephone and asked for AASIS number. Confirmation of other demographic information may be obtained at that time if the Security Gateway Administrator deems it appropriate.

If a match exists for non-ADH users, the ADMO will be contacted by telephone, will be asked for AASIS number, and will be asked to verify the request.

If validation of identity is not successful, the Security Gateway Administrator will notify the requesting ADMO that the access request is denied. If validation of identity is successful, the Security Gateway Administrator will re-direct the request to the appropriate Systems Administrators for processing.

Systems Security Functions

Application Access: Access to all applications connected through the ADH network must be processed through the integrated systems security gateway. Centers may impose additional identification and authentication requirements. Upon re-direct from the Gateway Administrator, such requirements will be managed by the Center's own Systems Administrators.

Network Services Access: Access to all ADH network services (to include but not limited to Network access, E-mail, Internet, etc.) must be processed through the integrated systems security gateway. All users must access ADH network services through the presentation and authentication of network credentials. Access to the Internet through the ADH network, without network authentication, is prohibited.

Logon Password Problems: Reports of logon password problems may be made directly to the Security Gateway Administrator (280-4357 or 800/941-9232). For Network access password issues, the Security Gateway Administrator will contact user by telephone, validate identity, and resolve the access issue. For password issues related to applications, following validation of identity, the Gateway Administrator will re-direct the report to the appropriate Systems Administrator. For password issues related to Center supported applications, following validation of identity, the Security Gateway Administrator will re-direct the report to the appropriate Center's Systems Administrator.

User Management

Access to all ADH network services and applications must be processed through the integrated systems security gateway. User access account requests and status changes are submitted on the ADH-359. This form must be completed in sufficient detail to satisfy basic security requirements and provide a complete audit trail of each user's history of access permissions. User access accounts must be attributable to an accountable person.

New User: ADMO's may submit requests for New User access. For non-ADH users, access accounts expire after a specified number of days defined by the CIO based on the business requirements of the group. Such accounts may be renewed by the Center ADMO.

Change User: ADMO's may submit requests for changes of a user's existing demographic data, change of types of access for network services, and changes of types of access for Center's applications. Users may submit requests, on their own behalf, for changes of demographic data.

Terminate User: For existing users, ADMO's may submit requests for termination of access. Termination of access will also occur on the basis of AASIS personnel data extracts. For non-ADH users, ADH has no means of checking personnel data, so it is particularly important that ADMO's actively report terminations of systems access. In addition, for non-ADH users access accounts expire after a specified number of days defined by the CIO based on the business requirements of the group.

Transfers Between Location or Centers: User change of location is reported by submitting an ADH Systems Security Access Request (ADH-359). Transferring or relocating ADH users will retain only their network credentials and e-mail access. The receiving ADMO must ensure the ADH-359 indicates: (1) change of user's network and applications access privileges for security purposes, (2) change of user's demographic information for access audit purposes, and (3) change of user's Center/work unit for network cost accountability purposes.

REMOVABLE AND PORTABLE STORAGE MEDIA

Introduction

- A. This policy establishes Arkansas Department of Health (ADH) procedures for the use of all removable and portable storage media, especially Universal Serial Bus (USB) devices, throughout the Department. The provisions of this policy are applicable ADH wide and apply to all employees, including contract workers.
- B. Information contained on such devices can be easily compromised if the device does not have adequate protective features. In addition, removable storage media can introduce malicious code to the ADH network via USB ports; consequently, their use must be controlled.
- C. The overall intent of this policy is not to restrict the use of technology but rather to provide directive for safe, secure, and appropriate use of such applications.

DEFINITION

- A. Removable and portable storage media or "media" means any media that can:
 - store data digitally,
 - can be removed from the device which uses the media, and transported to other locations, or
 - portable devices that have the capability to store data digitally and/or provide access to ADH systems.

Examples include, but are not limited to, all non-desktop computing devices (lap tops), personal digital assistants, blackberry phones, cell phones capable of data storage, floppy disks, CDs, DVDs, USB portable drives (thumb, flash, zip, jump, pen, etc), portable music players (iPods, zunes, any mp3 player, etc.), zip disks, jaz cartridges, backup storage tapes, portable (external) hard drives, and all types of memory cards or sticks.

Policy:

- A. ADH data may only be stored on ADH issued media.
- B. ADH data may not be stored on personal non-ADH issued media.
- C. Non-ADH media cannot be used on ADH equipment unless approved by the CIO.
- D. All ADH data transferred to a portable storage media must be classified pursuant to State of Arkansas Department of Information Systems Data and System Security Classification Standard (Document SS-70-001). This standard applies Criticality and Sensitivity levels to data. A summary of these levels is listed in this policy; however, the user must refer to the actual SS-70-001 document for application. To access the SS-70-001, go to http://www.dis.arkansas.gov/poli_stan_bestpract/standards.htm.

1. Criticality Levels

- a. **LEVEL 1 – NOT CRITICAL:** These data and systems are necessary to state government but short-term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of Arkansas' citizens.
- b. **LEVEL 2 – CRITICAL:** These data and systems are required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the data and systems can be restored.
- c. **LEVEL 3 – EXTREMELY CRITICAL:** These data and systems are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe. These data and systems also require restoration of the original facilities to be able to resume business.

2. Sensitivity Levels

- a. **LEVEL A - UNRESTRICTED:** Unrestricted data is characterized as being open public data with no distribution limitations and to which anonymous access is allowed. These data elements form information that is actively made publicly available by state government. It is published and distributed freely, without restriction. It is available in the form of physical documents, such as brochures, formal statements, press releases, reports that are made freely available, and in electronic form, such as internet web pages and bulletin boards accessible with anonymous access. The greatest security threat to this data is from unauthorized or unintentional alteration, distortion, or destruction of this data. Security efforts appropriate to the criticality of the system containing this data must be taken to maintain its integrity. Examples of data at this sensitivity level include many Agency public websites, newsletters, and presentations that do not contain Level B or higher data.
- b. **LEVEL B - SENSITIVE:** These data elements are the information that is made available through open records requests or other formal or legal processes. This category includes the majority of the data contained within the state government electronic databases. Direct access to this data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties. Security threats to this data include unauthorized access, alteration and destruction concerns. Examples include but are not limited to: most data elements in state personnel records, building code violations data, driver history records, collective bargaining data, employment and training program data, federal contracts data, firearm permits data, historical records, repository data, real estate appraisal data, occupational licensing data, and personnel data.

- c. **LEVEL C - VERY SENSITIVE:** Data classified as being very sensitive is only available to internal authorized users and may be protected by federal and state regulations. Very sensitive data is intended for use only by individuals who require the information in the course of performing job functions. These data elements include those protected by federal and state statute or regulation. Access to these data elements is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties. These are the data elements removed from responses to information requests for reasons of privacy. Security threats to this data include violation of privacy statutes and regulations in addition to unauthorized alteration or destruction. If this data were accessed by unauthorized persons, it could cause financial loss or allow identity theft. Unauthorized disclosure could provide significant gain to a vendor's competitors. Examples include but are not limited to: social security numbers, most home addresses, attorneys' files, comprehensive law enforcement data, domestic abuse data, educational records, foster care data, health and medical data, library borrower's records, signature imaging data, welfare records/data, credit card numbers, competitive bids, civil investigative data, criminal history data, economic development assistance data, food assistance programs data, head start data, juvenile delinquent data, counselors' data, and trade secrets data.
- d. **LEVEL D - EXTREMELY SENSITIVE:** Data classified as being extremely sensitive is data whose disclosure or corruption could be hazardous to life or health. These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health or safety repercussions. Very strict rules must be adhered to in the usage of this data. Examples of this data include, but are not limited to, the contents of state law enforcement investigative records and communications systems.
- e. Data with a Criticality Level of 1 and a Sensitivity Level of A may be placed on an unencrypted device. This is mainly for convenience of distribution, i.e. newsletters, press releases, presentations of a general nature (not containing sensitive data).
- f. All other data placed on removable and/or portable storage media must be encrypted with ADH approved encryption technology and use of a complex password.
- g. Blackberry phones, cell phones, and personal digital assistants must have encryption options turned on if available. If the device does not offer an encryption option, then password protection or key lock features must be turned on.

- h. All removable and/or portable storage media must be secured in locked facilities when not in use or when not being transported.
- i. Employees who have been issued removable and portable storage media are responsible for the security of the device and the data on the device. Any software that allows the device to be encrypted will not be removed by the user. Any missing removable and portable storage media must be reported immediately on an Occurrence Report (AS-8) and a copy sent to the ADH CIO.
- j. USB drives must be requisitioned thru the ADH CIO.
- k. The ADH CIO will place an encrypted file on each USB drive containing tracking number, the date issued, and other data as deemed necessary by the ADH CIO. The ADH CIO will keep a master record on each device with information to trace the device back to user.
- l. The ADH CIO will keep a log of this information on each USB drive and will periodically audit random drives to ensure that the drive is secure (not missing), and that the data on the drive adheres to this policy.
- m. All removable and portable storage media that is no longer useable or no longer functional must be securely transported to the ADH CIO for destruction.

INTERNAL INTRANET WEBSITE OPERATION AND MAINTENANCE

I. Policies:

General Policy Statement

The ADH Intranet Website is designed to:

- Make information accessible to all employees at the same time through one unique interface.
- Serve as a platform to facilitate daily work of all employees.
- Assist in building an Agency culture based on the values of sharing, innovation and collaboration.
- Enable Agency Centers to work together better by providing practical tools and real-time information.

See the E-Mail Usage Policy and the Information Systems Security Access policy in this Volume for specific policy provisions related to:

- e-mail,
- world wide web,
- Internet and Intranet acceptable use, and
- information systems security and access.

Standards

All pages within the ADH Intranet Website (<http://healthycolleagues/>) must meet the following standards:

- Be easy to use.
- Contain relevant, up-to-date content.
- Be created only by entities which are officially affiliated with the Agency.
- Link only to outside sites that are approved by the Center (non-governmental websites should have a disclaimer statement included).
- Relate to the Agency's mission.
- Comply with copyright laws and other state/federal laws that may apply (see "Copyrights and Trademarks" in this policy).
- Contain no personal pages for individuals (these are not considered Agency website pages and are not linked to the Agency's Intranet website).
- Identify at the bottom of each page the name of the author or responsible party, an ADH telephone number, an e-mail address and the date the page was last modified.
- Meet design and technical specifications established by the ADH Internal Communications Team and endorsed by the Agency's Internet Committee (see "Guidelines for Intranet Page Layout and Design" in this policy).

Content Management Roles and Responsibility

The Internal Communications Team is responsible for the ADH official Intranet and serves as its Website Manager.

- Each Center/work unit selects the Content Manager responsible for updating information for its specific Intranet pages. The Content Manager's name is submitted to the Internal Communications Team. If a new Content Manager is named, Centers notify the Internal Communications Team.
- Content Managers review their specific Intranet pages and content provided by Content Providers in their Centers that has been approved by Center Directors or their designees.
- The Internal Communications Team, as Website Manager, builds/constructs all new pages and posts approved additions, revisions or updates for the Intranet provided by Content Managers.
- Content Managers are provided training by the Internal Communications Team. Where required or requested, Content Managers for areas on the Intranet that require frequent updates and additions are provided secure access to their specific site to update, edit and post information. Otherwise, the Internal Communications Team posts updates and new information as requested by Content Managers.
- Centers and Content Managers are responsible for the ongoing review of their pages to ensure that they meet the criteria established by the ADH in this policy.
- Content Providers are responsible for making updates to any documents linked to the website and providing those documents to the Content Managers.
- Content Managers must assure that all information on their pages is up-to-date. Information that is more than one month old may be purged by the Internal Communications Team after contacting the Content Manager.
- Content Managers must make a good faith effort to ensure that:
 - The data does not duplicate or contradict other information published by ADH.
 - The information has been coordinated with the appropriate parties.
 - Materials developed for electronic dissemination are thoroughly checked for factual accuracy, data verification, misspellings, syntax, and typographical errors.

Copyrights and Trademarks

Content Managers must ensure that their pages comply with federal copyright laws.

- Copyright status must be verified and appropriate licenses or permissions obtained for all materials not created directly by ADH employees, such as text obtained from external sources, service marks, artwork and computer software.
- Proper reference should be given to all trademarks and logos by designating them with the © and ™ markings. Web authors should consult ADH Legal Services about the copyright status of documents, graphics, databases, etc., hosted on the ADH Intranet site.

Guidelines for Intranet Page Layout and Design

Website construction and design for the Agency Intranet will follow the style sheets developed by the Internal Communications Team and provided to each Content Manager. These style sheets are to be followed in order that the appearance and functionality for the entire Intranet site are consistent, professional and user-friendly. Some of the recommended website design standards that are followed on this website include:

- Using light-colored backgrounds.
- Using black as the preferred color for body copy to provide a high contrast.
- Avoiding underlining items unless they are hypertext links.
- Setting the page width so that graphics and/or text will display on most monitors without horizontal scrolling, and information can be printed on standard paper without cutting off the right side.
- Keeping the graphic content to a minimum to optimize page-loading speed.
- Limiting the use of animated graphics due to accessibility concerns.
- Including a text equivalent (“alt text”) for all images, including image maps.
- When using image maps, including the same links in a text form.
- Using text for navigation rather than graphics, whenever possible.
- Indicating the file size and type when linking to large images, audio or video.
- When linking to a non-HTML document, indicating the file type being linked to and providing a link to a free viewer, if possible.
- Not posting pages or adding them to navigation that are “under construction” until the pages are complete.

Submitting and Posting General Information to the Agency’s Intranet

The Internal Communications Team can also assist in distributing messages and general information that need to be sent which affect all employees statewide and are business-related. These may be posted on the Agency’s internal website and/or they may be sent as an ADH-All e-mail.

- Employees may request business-related information to be posted to the employee news, events and recognition sections of the Intranet.
- Articles or other information should be submitted to the Internal Communications Team with adequate advance notice to the time posting is desired.
- Information, including any attachments, should be previously reviewed and approved by the Center.

II. Procedures:

A. Adding New Materials to the Agency’s Intranet

Responsibility

Content Provider

Action

Presents concept to Center.

<u>Responsibility</u>	<u>Action</u>
Content Provider	<u>If approved</u> , completes content development and e-mails digital files for approval/disapproval to Content Manager for his/her Center.
Content Manager	<u>If approved</u> , e-mails digital files to Website Manager for approval/disapproval.
Content Provider	<u>If the Center does not have a designated Content Manager</u> , submits the approved material to the Website Manager to be posted.
Website Manager	<u>If approved</u> , creates a mock-up and submits link for review and final approval to Content Provider and Content Manager. <u>If approved</u> , makes the new content “live” and accessible to website visitors.

B. Revisions to Intranet Site Pages

<u>Responsibility</u>	<u>Action</u>
Content Provider	<u>If approved</u> , completes content development and e-mails digital files for approval/disapproval to Content Manager for his/her Center.
Content Manager	<u>If approved</u> , e-mails digital files to Website Manager for approval/disapproval.
Content Provider	<u>If the Center does not have a designated Content Manager</u> , submits the approved material to the Website Manager to be posted.
Website Manager	<u>If approved</u> , creates a mock-up and submits link for review and final approval to Content Provider and Content Manager. <u>If approved</u> , makes the new content “live” and accessible to website visitors.

EXTERNAL INTERNET WEBSITE OPERATION AND MAINTENANCE

I. Policies:

General Policy Statement

The ADH website is designed to:

- Deliver Information to a broad audience regarding, but not limited to, ADH services and programs, health or safety issues, public policies or issues of interest, regulations, licenses, and public health data and information.
- Support vendors or public health professionals.
- Reduce support and customer service costs (paperwork, printing and mailing costs).
- Recruit new employees.
- Provide links to additional information beyond the ADH site.
- Provide for successful use of online tools to support professional license renewal, a means to sign up to receive ongoing information from ADH, receipt of ongoing feedback about the site and a means for internet site visitors to download reports or forms.
- Support research.

See the E-Mail Usage Policy and the Information Systems Security Access policy in this Volume for specific policy provisions related to:

- e-mail,
- world wide web,
- Internet and Intranet acceptable use, and
- information systems security and access.

Standards

All pages within the ADH Website (www.healthy.arkansas.gov) must meet the following standards:

- Be easy to use.
- Contain relevant, up-to-date content.
- Be created only by entities which are officially affiliated with the Agency.
- Link only to outside sites that are approved by the Agency (non-governmental websites should have a disclaimer statement included).
- Relate to the Agency's mission.
- Comply with copyright laws and other state/federal laws that may apply.
- Contain no personal pages for individuals (these are not considered Agency website pages and are not linked to the Agency's website).
- Meet design and technical specifications established by the ADH Internet Committee and the state website guidelines established by the state Department of Information Services and by the Information Network of Arkansas pertaining to all state agency websites.

Website Construction, Design

The Arkansas Department of Health (ADH) Internet website uses common templates implemented through the enterprise content management system (CMS) provided by the Information Network of Arkansas (INA). ADH website guidelines and standards require use of the ADH templates to produce a similar experience throughout the website. The ADH Internet website meets and exceeds Arkansas's accessibility standards.

Some of the recommended website design standards that are followed on this website include:

- Using light-colored backgrounds.
- Using black as the preferred color for body copy to provide a high contrast.
- Avoiding underlining items unless they are hypertext links.
- Setting the page width so that graphics and/or text will display on most monitors without horizontal scrolling, and information can be printed on standard paper without cutting off the right side.
- Keeping the graphic content to a minimum to optimize page-loading speed.
- Limiting the use of animated graphics due to accessibility concerns.
- Including a text equivalent ("alt text") for all images, including image maps.
- When using image maps, including the same links in a text form.
- Using text for navigation rather than graphics, whenever possible.
- Indicating the file size and type when linking to large images, audio or video.
- When linking to a non-HTML document, indicating the file type being linked to and providing a link to a free viewer, if possible.
- Not posting pages or adding them to navigation that are "under construction" until the pages are complete.

Content Management

The Arkansas Department of Health Internet Committee, comprised of representatives throughout the Agency, is responsible for the ADH Internet in the areas of management, design and content maintenance. The roles established by the Committee are Content Provider, Content Manager and Website Manager. "Content" includes text, graphics and linked files. Each ADH Center has a Content Manager, as well as Content Providers designated by each work unit. Web content is approved at the Center administration level, and the content is then forwarded by the Content Manager to the Website Manager to make it viewable to the public on the website.

Each role is granted permission to perform certain functions within the content management system. These functions have been established by INA through a defined workflow based on software and website functionality and as a means to assure appropriate and adequate review of content before it is made public. This helps ensure the Department Internet website is a viable communications tool to assist the Department in its public health mission.

Content Management Roles and Responsibility

The Internal Communications Team is responsible for the ADH official Internet and serves as its Website Manager.

- Each Center/work unit selects the Content Manager responsible for updating information for its specific Internet pages. The Content Manager's name is submitted to the Internal Communications Team. If a new Content Manager is named, Centers notify the Internal Communications Team.
- Content Managers review their specific Internet pages and content provided by Content Providers in their Centers that has been approved by Center Directors or their designees.
- The Internal Communications Team, as Website Manager, builds/constructs all new pages and posts approved revisions or updates for the Internet provided by Content Managers.
- Content Managers are provided training by the Internal Communications Team.
- Centers and Content Managers are responsible for ongoing review of their pages to ensure that they meet the criteria established by the ADH in this policy.
- Content Managers must make a good-faith effort to ensure that:
 - The data does not duplicate or contradict other information published by ADH.
 - The information has been coordinated with the appropriate parties.
 - Materials developed for electronic dissemination are thoroughly checked for factual accuracy, data verification, misspellings, syntax, and typographical errors.
- Content Providers are responsible for making updates to any documents linked to the Internet site and providing those documents to their Content Managers.

Copyrights and Trademarks

Content Managers must ensure that their pages comply with federal copyright laws.

- Copyright status must be verified and appropriate licenses or permissions obtained for all materials not created directly by ADH employees, such as text obtained from external sources, service marks, artwork and computer software.
- Proper reference should be given to all trademarks and logos by designating them with the © and ™ markings. Web authors should consult the ADH Legal Services about the copyright status of documents, graphics, databases, etc., hosted on the ADH Internet site.

Ancillary Websites

All websites for ADH programs and services, including ancillary websites operated by ADH programs or services at the time this policy is put into force, must:

- be part of the overall Department website,
- be accessed through its URL address, and
- comply with all ADH website policies and procedures.

This includes any website for which ADH resources are expended, including funds, grant money or staff time.

If an ancillary website has a separate or pre-existing URL, the ancillary website will become part of the overall ADH Internet site by means of a URL “re-direct.” The ADH Webmaster, INA or other information services technical resources will provide assistance to accomplish a re-direct, as needed. Using the re-direct function, visitors to an existing ancillary website who use that site’s URL are virtually and transparently “redirected” to the program pages at the www.healthy.arkansas.gov URL.

Some ancillary Websites are maintained in partnership with other public health organizations. In those cases, exceptions to some website policy provisions may be necessary. These are considered on a case-by-case basis.

No new ancillary websites operated by ADH programs or service areas will be created without specific permission/approval of the ADH Internet Committee.

II. Procedures:

A. Adding New Materials on the Agency’s Website

<u>Responsibility</u>	<u>Action</u>
Content Provider	Presents concept to Center. <u>If approved</u> , completes content development and e-mails digital files for approval/disapproval to Content Manager for his/her Center.
Content Manager	<u>If approved</u> , e-mails digital files to Website Manager for approval/disapproval.
Content Provider	<u>If the Center does not have a designated Content Manager</u> , submits the approved material to the Website Manager to be posted.
Website Manager	<u>If approved</u> , creates a mock-up and submits link for review and final approval to Content Provider and Content Manager. <u>If approved</u> , makes the new content “live” and accessible to website visitors.

B. Revisions to Internet Site Pages

<u>Responsibility</u>	<u>Action</u>
Content Provider	<u>If approved</u> , completes content development and e-mails digital files for approval/disapproval to Content Manager for his/her Center.
Content Manager	<u>If approved</u> , e-mails digital files to Website Manager for approval/disapproval.
Content Provider	<u>If the Center does not have a designated Content Manager</u> , submits the approved material to the Website Manager.
Website Manager	<u>If approved</u> , creates a mock-up and submits link for review and final approval to Content Provider and Content Manager. <u>If approved</u> , makes the new content “live” and accessible to website visitors.

HIPAA PRIVACY/SECURITY POLICY
HIPAA PRIVACY REQUIREMENTS FOR E-MAIL AND FACSIMILE SERVICES

Policies:

GENERAL

- A. Electronic mail (e-mail), Internet access, and facsimile (FAX) services are made available to ADH staff for the purpose of facilitating the conduct of ADH business and enabling the efficient communication of information and data. These services must be used by ADH staff in a manner that conforms to all applicable state and federal laws, regulations and policies. Each ADH employee is responsible for ensuring the privacy of protected health information (PHI).

E-MAIL

- A. Approved Methods of Conveyance: All e-mail messages containing protected health information (PHI) as defined in this policy and sent by ADH staff to destinations within the state's e-mail system must be sent encrypted. Sending e-mail messages containing PHI to destinations outside the state's e-mail system is not secure and is prohibited, unless the e-mail can be encrypted. If the message cannot be encrypted, it may be sent by FAX, employing the privacy safeguards outlined in this policy. Conveyance of large electronic files requires secure media sharing (password protected files on disk or CD) or conveyance by a secure transfer protocol. Consult with the Chief Information Officer (CIO) for assistance.
- B. Content Requirements: Any e-mail message generated by ADH staff that contains PHI must conform to the following requirements:
1. E-mail Subject Line: For messages containing PHI, the subject line must state, in whole or part, "CONTAINS PROTECTED INFORMATION."
 2. E-mail Addresses: E-mail messages may be sent, copied, or forwarded only to those persons who have a need to know the patient information. Global, group, or broadcast addresses should not be used when sending e-mail messages that contain PHI. The purpose of this requirement is to avoid inadvertent disclosure to addressees who lack a need to know the protected information.

3. E-mail Message: At the bottom of the message the following privacy warning must be displayed: "Confidentiality Notice: The information contained in this e-mail message and any attachment is the property of the State of Arkansas and may be protected by state and federal laws governing disclosure of private information. It may contain information that is privileged, confidential, or otherwise protected from disclosure. It is intended solely for the use of the addressee. If you are not the intended recipient, you are hereby notified that reading, copying or distributing this e-mail or the information herein by anyone other than the intended recipient is **STRICTLY PROHIBITED**. The sender has not waived any applicable privilege by sending the accompanying transmission. If you have received this transmission in error, please notify the sender by reply e-mail immediately, and delete this message and attachments from your system."
 4. Minimum Necessary Content: E-mail messages containing PHI must contain only the minimum necessary information to accomplish the purpose of the communication.
- C. Unsecured E-mail Requirements: When originating messages in the state's unsecured e-mail system (i.e., not Web Access), users are required to review messages and attachments and must expunge all information that may be defined as PHI. Such review is required not only for messages authored by the user, but also for forwarded messages and all the messages in the forwarded strings.
- D. User Hard Drives: Hard drives must also be protected from PHI disclosure. Use of Personal Folders (Microsoft Outlook) creates a file on the local hard drive which may be exposed to the Internet through the use of file sharing applications (e.g., Napster, Swapnut, Gnutilla, etc.) and the efforts of malicious hackers. Installation of third party file sharing applications is prohibited. ADH employees must expunge PHI from Personal Folders in their Outlook account.

FAX

- A. Approved Methods of Conveyance: All FAX messages containing protected health information (PHI) as defined in this policy and sent by ADH staff to any destination must be safeguarded for confidentiality and privacy in accordance with federal and state law, and must employ privacy safeguards outlined in this policy. FAXes may be sent only to a specific person for whom such release has been determined to be authorized. It should be established, by prior telephone contact, that a specific person is present to receive the transmitted FAX.
- B. Content Requirements: FAX messages must use a cover sheet with the word **CONFIDENTIAL** appearing in bold letters near the top of the form. Further, all such FAXes must include a statement regarding prohibition of disclosure of identifying PHI. The statement should read as follows:

- (1) "Prohibition of Rediscovery: This information has been disclosed to you from records that are confidential. You are prohibited from using the information for other than the stated purpose; from disclosing it to any other party without the specific written consent of the person to whom it pertains; and are required to destroy the information after the stated need has been fulfilled, or as otherwise permitted by law. A general authorization for the release of medical or other information is not sufficient for this purpose."

HIPAA TRAINING REQUIREMENTS

Policy:

Since ADH is a covered entity, the entire workforce must complete HIPAA Privacy and Security Training. All employees must review the Privacy/Security Policy in this Volume and sign the Employee Privacy/Security Policy Acknowledgment (AS-38) on their first work day.

Note: If a current employee has already signed an Employee Privacy Policy Acknowledgment (No Number) and it is on file, the employee does not have to sign an AS-38.

Each employee's supervisor ensures that the employee signs the AS-38 on his first work day and completes the additional, appropriate training listed below within the first month of employment:

Full-time/Part-time Employees:

HIPAA Web-Based Training
If IHS, also view the Beacon Health Video

Extra-Help Employees:

HIPAA Web-Based Training
Confidentiality Agreement (AS-32)
If IHS, also view the Beacon Health Video

Contract Employees:

Addendum Added to Contract
HIPAA Web-Based Training – Optional – depending on job duties
If IHS, also view the Beacon Health Video

Volunteers/Students:

HIPAA-Web-Based Training – Optional – depending on job duties
Confidentiality Agreement (AS-32) **(Must be 18 or older to sign agreement)**
If IHS, also view the Beacon Health Video

HIPAA PRIVACY/SECURITY POLICY INDIVIDUAL RIGHTS

Policies:

- A. HIPAA regulations provide specific rights to individuals. These rights are listed on the Privacy Notice (AS-30a) that is provided to all new patients/clients. Specifically, individuals have the right to request to:
- i. Receive a paper copy of the Privacy Notice. The patient may request a paper copy of the Privacy Notice from ADH at any time. (See the Privacy Notice policy in this Volume.)
 - ii. File complaints regarding violations by ADH of their privacy rights granted to them and created by HIPAA. (See the HIPAA Complaint policy in this Volume.)
 - iii. Inspect and/or copy their health information. A patient may request to inspect or have a copy of any part of his/her health record. ADH may charge a fee for the costs of copying, mailing, or other supplies associated with this request. (See Right To Inspect and Copy policy in this Volume.)
 - iv. Amend their health information. If a patient feels that the health information the ADH has created about him/her is incorrect or incomplete, he/she may ask ADH to amend that information. (See the Right to Request Amendment of Protected Health Information policy in this Volume.) The ADH may deny the request if requested to:
 - (a) amend information that was not created by the ADH;
 - (b) amend information that is not part of the health information kept by the ADH;
 - (c) amend information that is not part of the information which the patient would be permitted to inspect or copy; or
 - (d) amend information that is determined to be accurate and complete.
 - v. Request restrictions of their health information. The patient may request ADH to limit the use or disclosure of the patient's health information for treatment, payment, and health care operations or to certain individuals. ADH is not required by law to agree to this request. (See Right to Request Restrictions policy in this Volume.)
 - vi. Request confidential communication of their health information. The patient may request, in writing, that ADH communicate with him/her in a different way or to a different location, for example, using a different mailing address or calling the patient at a different phone number. (See Right to Request Confidential Communication policy in this volume.)

- vii. Obtain an accounting of disclosures of health information. The patient may request an accounting of disclosures of his/her health information. The accounting does not include disclosures for purposes of treatment, payment, health care operations; disclosures required by law for purposes of national security; disclosures to jails or correctional facilities, authorized disclosures, and any disclosures made prior to April 14, 2003. (See Right to Accounting of Disclosure of Protected Health Information policy in this Volume.)
- B. All requests must be directed to the Local Health Unit Administrator/IHS Administrator.
 - C. If there are difficulties in accommodating these requests, the Local Health Unit Administrator/IHS Administrator contacts the ADH Privacy Officer.
 - D. An individual may revoke an authorization to release his/her information, in writing, and the Agency will no longer release the information.

HIPAA PRIVACY/SECURITY POLICY MARKETING

Policies:

HIPAA MARKETING DEFINITIONS

A. HIPAA defines marketing as:

- (1) Communications about a product or service that encourages recipients of the communication to purchase or use the product or service.
- (2) Arrangements between an entity subject to HIPAA regulations (“covered entity”) and other entities whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service. Without the client’s authorization a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.

Examples of “marketing” communications requiring prior authorization are:

- (a) A communication from a hospital informing former patients about a cardiac facility, that is not part of the hospital, that can provide a baseline EKG for \$39, when the communication is not for the purpose of providing treatment advice.
- (b) A communication from a health insurer promoting a home and casualty insurance product offered by the same company.

It is also considered “marketing” when:

- (c) A health plan sells a list of its members to a company that sells blood glucose monitors, which intends to send the plan’s members brochures on the benefits of purchasing and using the monitors.
- (d) A drug manufacturer receives a list of patients from a covered health care provider and provides remuneration, then uses that list to send discount coupons for a new anti-depressant medication directly to the patients.

B. Pursuant to HIPAA, the following types of communications are **NOT** considered marketing:

- (1) Communications by a covered entity to an individual for the purpose of describing to that individual a health-related product or service that is provided by the covered entity, or included in the covered entity's plan of benefits; or
- (2) Communications by a covered entity to an individual as part of the treatment of the individual; or
- (3) Communications by a covered entity to an individual in the course of managing or coordinating treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.
- (4) Communications about government and government-sponsored programs do not fall within the definition of "marketing." A covered entity is permitted to use and disclose protected health information to communicate about eligibility for such programs as Medicare, Medicaid, or the State Children's Health Insurance Program (SCHIP).

Examples of communications that are not considered "marketing" are:

- (e) A hospital uses its patient list to announce the arrival of a new specialty group (e.g., orthopedic) or the acquisition of new equipment (e.g., x-ray machine or magnetic resonance image machine) through a general mailing or publication.
- (f) A health plan sends a mailing to subscribers approaching Medicare eligible age with materials describing its Medicare supplemental plan and an application form.
- (g) A pharmacy or other health care provider mails prescription refill reminders to patients, or contracts with a mail house to do so.
- (h) A primary care physician refers an individual to a specialist for a follow-up test or provides free samples of a prescription drug to a patient.
- (i) An endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient.
- (j) A hospital social worker shares medical record information with various nursing homes in the course of recommending that the patient be transferred from a hospital bed to a nursing home.

HIPAA MARKETING

- A. HIPAA specifically prohibits using or disclosing a client's protected health information (PHI) for marketing purposes, as defined above, unless:
- The client provides written authorization to use his/her PHI for marketing. If there is remuneration for use of the client's PHI, the authorization must state that remuneration is involved;
 - The communication occurs in a face-to-face encounter between the covered entity and the individual; or
 - The communication involves a promotional gift of nominal value.
- B. ADH will not use or disclose a patient's protected health information for marketing purposes except as allowed by federal and state law, including the Federal HIPAA Privacy Regulations.
- C. Minimum Necessary: Any and all uses or disclosure of PHI for marketing purposes in compliance with this policy will be limited to the minimum amount of information necessary to achieve the purpose of the use or disclosure.
- D. Business Associate Agreement Required: If ADH intends to disclose PHI to a third party for the purpose of the third party communicating with clients about the products or services of ADH, such disclosure does not constitute marketing communications and does not require patient authorization. Prior to such disclosure, ADH is required to enter into a written agreement with the third party restricting the third party's use of the PHI to communications on behalf of ADH and ADH's own products and services. The agreement will be a Business Associate Agreement (AS-4001).

Note: The use of a Business Associate Agreement will not take the place of a patient authorization in situations involving the use or disclosure of PHI to facilitate or conduct communications with patients about the products or services of others. This would include, for example, a situation where a company seeks access to a list of ADH patients or any other PHI which the company will use for its own marketing activities to promote its own products or services, regardless of whether the company is to use the PHI on behalf of ADH as well, and seeks to do so under the guise of a business associate relationship or agreement. This situation requires prior patient authorization.

HIPAA PRIVACY/SECURITY POLICY
MITIGATION AND SANCTIONS OF VIOLATIONS OF PRIVACY RIGHTS

Policies:

MITIGATION

- A. As required by HIPAA, the ADH will mitigate any known harmful effect(s) of uses or disclosures of protected health information made by ADH or its business associates in violation of HIPAA or ADH policy related to privacy rights granted by HIPAA.
- B. Mitigation means taking all appropriate actions listed below if an ADH client's HIPAA privacy rights have been violated:
- (1) Notifying any unintended or unauthorized recipient(s) of protected health information (including by e-mail or fax) and requesting that they disregard, keep confidential, not reveal, and discreetly dispose of said information.
 - (2) Investigating the causes of the disclosure.
 - (3) Taking corrective action including:
 1. Sanctions for violation of ADH HIPAA Privacy/Security policies.
 2. Training or retraining as necessary.
 3. Correcting faulty processes.

SANCTIONS

- A. The HIPAA privacy rule requires that ADH have and apply appropriate sanctions against members of its workforce who fail to comply with ADH HIPAA Privacy/Security policies.
- B. Sanctioning personnel for violation of this policy will be pursuant to ADH policies pertaining to policy violation.
- C. Sanctions for violation of ADH HIPAA Privacy/Security policies will not apply to employees who disclose PHI if:
1. The employee, acting as a "whistleblower," believes in good faith that the ADH has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the services provided by ADH potentially endanger patients, workers, or the public; and

1. The disclosure is to an agency or authority authorized by law to investigate or oversee the conduct of ADH, or
 2. The disclosure is to an attorney retained by the employee in order to determine the legal options of the employee when disclosing information as described in this section.
2. The employee files a complaint with the Secretary of DHHS pursuant to the HIPAA Regulations, and the PHI disclosed is a necessary part of that complaint.

DOCUMENTATION

- A. All mitigation and sanction actions associated with a violation of ADH HIPAA Privacy/ Security policies will be documented and retained on file by the ADH Privacy Officer/ Program Consultant.

HIPAA PRIVACY/SECURITY POLICY PRIVACY NOTICE

Policies:

GENERAL

ADH is required to provide clients with whom it has a “direct treatment relationship” with a Privacy Notice (AS-30a) that describes how ADH uses and discloses protected health information (PHI), describes ADH’s legal duties with respect to PHI, and informs the client of his/her rights pertaining to PHI. HIPAA regulations divide treatment relationships into those that involve direct interactions between providers and patients, and those that involve indirect interactions.

PRIVACY NOTICE

The Agency is required to provide the Privacy Notice (AS-30a) to all clients, except for WIC Program Only clients, during their first visit to the clinic.

- (1) In emergency situations, the provision of the Privacy Notice and its written Acknowledgment of Receipt (AS-30b) may be given as soon as reasonably practicable after the emergency treatment situation.
- (2) A copy of the AS-30a must be given to the client any time it is requested.
- (3) If the AS-30a is revised, the revisions must be made available to the patient during his/her next visit if requested.
- (4) Reasonable measures, such as translation or reading of the AS-30a, must be provided if requested.
- (5) The ADH must make the Privacy Notice available to anyone who asks for a copy. If the person requesting the Privacy Notice is not a patient or client, then an AS-30b is not needed.
- (6) In each ADH location that provides service to individuals, the ADH must post the Privacy Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the ADH to be able to read the Privacy Notice.

PRIVACY NOTICE ACKNOWLEDGMENT

ADH employees providing a copy of the Privacy Notice to clients must request the client to sign an Acknowledgment of Receipt (AS-30b). The AS-30b indicates that the Privacy Notice was given to the client.

- i. If the patient refuses to sign the AS-30b, note such in the “For Official Use Only” section of the AS-30b by signing and dating the form.
- ii. If the Privacy Notice is revised and the patient requests a copy of the revised Privacy Notice, then another AS-30b must be obtained from the client.
- iii. Exception: For Immunization Only patients, stamp the HIPAA Privacy Notice Acknowledgment statement on the IMM-1, Comments section, and obtain the signature on the IMM-1, instead of the AS-30b.

DOCUMENTATION REQUIREMENTS

- A. A copy of the AS-30a and each subsequent revision will be retained for six years by the ADH HIPAA Office.
- B. A copy of the AS-30b will be retained by each LHU issuing the AS-30a for six years.

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO ACCOUNTING OF DISCLOSURE OF PROTECTED HEALTH INFORMATION

I. Policies:

1. ACCOUNTING OF DISCLOSURE OF PROTECTED HEALTH INFORMATION

- A. ADH clients (and their legal representatives) have a right to request an accounting of PHI disclosures that ADH has made for a period of up to six years previous to the date of request. It is ADH policy that all disclosures of client PHI (subject to accounting and tracking) will be recorded on the Accounting Of Disclosures Of Protected Health Information (AS-31).
- B. Upon receipt of a request for an accounting of PHI disclosures, ADH will have a maximum of 60 calendar days to compile the accounting of disclosures and respond to the client request. If ADH is unable to comply with the client's request for an accounting of PHI disclosures within 60 calendar days, ADH may make a one-time extension of the timeframe for response by 30 calendar days.
- C. The accounting of PHI disclosures must include:
 - (1) The date of the disclosure.
 - (2) The name and address, if known, of the person or entity that received the disclosed PHI.
 - (3) A brief description of the information disclosed.
 - (4) A brief statement of the purpose of the disclosure that reasonably informs the client of the basis for the disclosure, or, in lieu of such statement, a copy of the client's written request for the accounting of disclosures.

2. DISCLOSURES SUBJECT TO TRACKING AND ACCOUNTING

- A. Disclosures subject to tracking and accounting include, but are not limited to, the following:
 - (1) Abuse Reports. PHI provided pursuant to mandatory abuse reporting laws to an entity authorized by law to receive abuse reports.
 - (2) Audit Review. PHI provided from a client record in relation to an audit or review of a provider or contractor or disclosures to insurers for claims investigations.

- (3) Health and Safety. PHI provided to avert a serious threat to the health and/or safety of a person or persons.
- (4) Licensee/Provider. PHI provided from a client record in relation to licensing, regulation or certification of a provider or licensee involved with the provision of care or services to the client.
- (5) Legal Proceedings. PHI ordered to be disclosed pursuant to a court order.
- (6) Law Enforcement Official/Court Order. PHI provided to a law enforcement official pursuant to a court order.
- (7) Law Enforcement or Other Official/Deceased. PHI concerning a deceased client provided to law enforcement official, medical examiner or other official for the purpose of identifying a deceased person, determining the cause of death, or for other reasons authorized by law.
- (8) Law Enforcement Official/Warrant. To the extent permitted by law, PHI provided to a law enforcement official concerning a fleeing felon or client subject to an arrest warrant.
- (9) Public Health Authority. PHI provided to public health authorities for the reporting of disease or injury or for the conduct of a public health study or investigation.
- (10) Public Record. PHI disclosed pursuant to a Public Record request without the client's authorization.
- (11) Research. PHI provided for research purposes using a waiver of authorization provided by an Institutional Review Board (IRB).
- (12) Required by Law. Disclosures that result from a requirement from another federal or state law or regulation.
- (13) Government Entity. Disclosures to any government entity or health oversight agency, unless otherwise exempted.

3. DISCLOSURES NOT SUBJECT TO TRACKING AND ACCOUNTING

A. Disclosures not subject to tracking and accounting include:

- (1) Disclosures for Treatment, Payment and Operations (TPO).
 - (a) Treatment – the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.

- (b) Payment – activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
- (c) Operations – functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

- (2) Disclosures to the client.
- (3) Disclosures made pursuant to a valid authorization of the client.
- (4) Disclosures or uses made subject to the client's opportunity to object, including:
 - (a) Use to maintain a facility directory and disclosures from the directory to clergy and persons who ask for the individual by name.
 - (b) Use and disclosure to persons involved with the client's care, payment for services, or for notification of general condition or death to persons responsible for the care of the client.
 - (c) Disclosures for disaster relief purposes.
- (5) Use and disclosures for national security and intelligence activities.
- (6) Use and disclosures to correctional institutions and other law enforcement custodial situations.
- (7) Disclosure as part of a limited data set, which excludes direct identifiers for research, public health, or health care operations.
- (8) Disclosures which occurred prior to the effective date of HIPAA Privacy requirements.
- (9) Incidental disclosures.
- (10) Use of PHI within ADH.

4. REQUESTS FOR ACCOUNTING OF PHI DISCLOSURES

- A. Clients (or their legal representatives) may make their requests by completing a Request for an Accounting of Disclosures of Protected Health Information (AS-33). A request for an accounting of PHI disclosures must identify the record holder and the period of time covered by the request. When a request for an accounting is received:
- (1) The ADH staff member receiving the request for an accounting must document the identity of the requestor by identification badge, driver's license, written statement of identity on Agency letterhead, or similar proof. When an oral request is received in person or by phone, ADH will confirm the request with a written statement describing the request and obtain a client signature for authentication.
 - (2) When the request for accounting is documented and accepted, the client will be provided an acknowledgement statement indicating when he/she can expect to receive an accounting. An Acknowledgement of Request for Accounting of Disclosure or Amendment to PHI (AS-4009) will be used.
 - (3) The client's health record will be reviewed to determine if PHI disclosures have occurred during the time period covered by the client's request. This will be accomplished through manual review of the Accounting of Disclosures of Protected Health Information (AS-31). If accounting of disclosures cannot be completed within 60 days of the request, the client will be notified using an Accounting of Disclosures Response Letter (AS-34).
 - (4) When a list of disclosures has been compiled, the AS-34 will be completed and a copy of the client's AS-31 will be forwarded to the client.
 - (5) Client requests for accountings of PHI disclosures will be filed in the client's health record and maintained for a period of six years from the date the request is completed.
 - (6) The accounting must be documented on the Accounting of Disclosures of Protected Health Information (AS-31). Individuals may request an accounting for up to six years prior to the date on which the accounting is requested. The earliest possible beginning date is April 14, 2003.
 - (7) The Agency provides the first accounting in any 12 month period without charge. ADH may charge for additional copies.

(8) If the client has any questions concerning the content of the accounting, he/she will be referred to the ADH Privacy Officer/Program Consultant at:

Arkansas Department of Health
ADH Privacy Officer/Program Consultant
4815 W. Markham Street, Slot 31
Little Rock, Arkansas 72205-3867
Phone - 501-661-2000

5. SUSPENSION OF ACCOUNTING OF PHI DISCLOSURES

The Agency must temporarily suspend an individual's right to receive an accounting provided to a health oversight agency or law enforcement official if provided a written statement indicating the accounting would likely impede the Agency's activities. The statement must specify the timeframe the suspension is required. If the agency or official requests a suspension orally, ADH must document the statement, including the identity of the agency or official making the statement, temporarily suspend the client's right to an accounting of disclosures subject to the statement and limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

II. Procedures:

Responsibility

Action

Client

Completes a Request for an Accounting of Disclosures of Protected Health Information (AS-33). Retains AS-33 in client's file.

LHU Administrator/IHS
Administrator/Designee

Documents the identity of the requestor by identification badge, driver's license, written statement of identity on Agency letterhead, or similar proof.

Notifies the client of receipt of the request using the Acknowledgement of Request for Disclosure or Amendment to PHI (AS-4009). Retains a copy of the AS-4009 in the client's file.

Notifies the ADH Privacy Officer/Program Consultant immediately after the request for accounting has been verified.

Responsibility

Action

LHU Administrator/IHS
Administrator/Designee

Determines if access is granted based on
timeframe and/or disclosure exceptions.

Note: Individuals may request an
accounting for up to six years.
(The earliest possible beginning
date is April 14, 2003.)

If request is granted:

Within 60 days of receipt of the request,
sends client an Accounting of Disclosures
Response Letter (AS-34) and attaches a
copy of the Accounting of Disclosures of
Protected Health Information (AS-31) and
any blanket disclosure statements.
Provides a copy of both to the ADH Privacy
Officer/Program Consultant.

If request cannot be granted within 60
days from date of client's request,
notifies client prior to 60 day limit
using AS-34. Provides a copy to the ADH
Privacy Officer/Program Consultant.

If request is denied:

Determines access is denied, completes
Accounting of Disclosures Response Letter
(AS-34), sends a copy to individual
making request within 60 days of the
request, and sends a copy to the ADH
Privacy Officer/Program Consultant.

If request is suspended:

Notifies client that his/her request has
been suspended by sending the client an
Accounting of Disclosures Response Letter
(AS-34) and sends a copy to the ADH
Privacy Officer/Program Consultant.

Note: In all cases, a copy of the AS-34
is retained in the client's file.

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO INSPECT AND COPY

I. Policies:

- A. Individuals have the right to inspect and obtain a copy of their health information. This request may include medical, billing, or health care payment information, but does not include information that is needed for civil, criminal, or administrative actions or proceedings or psychotherapy notes. The Agency may charge a fee for the costs associated with an individual's request.
- B. All requests for clients to inspect or obtain a copy of their health information must be in writing, preferably using the Authorization to Disclose or Release Health Information (AS-4000).
- C. ADH must provide access or deny the request no later than 30 days following the receipt of a request when the PHI is maintained or accessible on-site. Within 30 days of a request, individuals must have appointments scheduled to access their PHI, copies of PHI given or mailed to them, or be sent a denial notice disallowing access.
- D. If the PHI is not accessible on-site, the covered entity must provide access or deny access no later than 60 days from receipt of such a request.
- E. ADH may delay the response to the request for access only once by 30 days as long as a written statement of the reasons for the delay and the date the covered entity will take action on the request is provided to the individual within the above deadlines. This makes the maximum time to respond to be 60 days to provide access or deny a request for on-site PHI and 90 days for off-site PHI.
- F. ADH may deny an individual's request to inspect and obtain a copy of his/her protected health information (PHI) for the following reason(s):
 - A. ADH does not possess the information requested. If ADH knows where the information resides, it must inform the client.
 - B. Requested information was/is being compiled in anticipation of, or for use in, a civil, criminal or administrative action or proceeding
 - C. Requested information is subject to or exempted by the Clinical Laboratory Improvements Amendments (CLIA) of 1988.
 - D. Requested information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

- E. Requested information was/is being created or obtained in the course of ongoing research that includes treatment and the client agreed to the denial of access when he/she consented to participate in the research. (The client's right of access will be reinstated upon completion of the research.)
 - F. ADH may choose not to release Psychotherapy notes (as defined by HIPAA).
 - G. The requested information is contained in records subject to the federal Privacy Act, 5 U.S.C. §552a, and this denial meets the requirements of that law. (The Privacy Act of 1974 protects personal information about individuals held by the federal government.)
 - H. A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger the individual's or another's life or physical safety.
 - I. The requested information makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.
 - J. If the requestor is the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the requested information should not be provided to the personal representative.
- G. If access to requested information has been denied under items F.8, F.9, or F.10 listed in this policy, the client has the right to a review of the denial by ADH's Patient Care Team members who did not participate in this denial by submitting a written request to the ADH Privacy Officer/Program Consultant.

II. Procedures:

Responsibility

Action

Client

Submits written request or completes an Authorization to Disclose or Release Health Information (AS-4000) to inspect/obtain a copy of his/her protected health information and provides to the LHU.

Local Health Unit Administrator/
In-Home Services Administrator/
Designee

Consults with PHN/HHN (Home Health Nurse) (if LHU Administrator is not a PHN/HHN) to determine if access is granted or denied. (See Copy/Inspect Denial Letter (AS-35) to make determination.)

Responsibility

Action

Local Health Unit Administrator/
In-Home Services Administrator/
Designee

If request is granted:

Provides a copy to the individual PHN/HHN to determine if access is within 30 days of receipt of the request in the requested format, if possible; if not, in a readable hard copy form.

Note: The time limit may be extended an additional 30 days if the date by which the copies will be sent and a written statement of the reason for the delay is sent to the individual within the first 30 days.

Arranges a convenient time and place for individual to inspect or obtain copy, or mails the copy at the individual's request. Charges for copying according to the Record Maintenance Fee, Record Duplication, in the Funds Control Section of the Financial Management Volume. Note: If individual inspects record, it must be in the presence of the Local Health Unit Administrator/IHS Administrator/designee.

If request is denied:

Completes Copy/Inspect Denial Letter (AS-35) and sends a copy to individual within 30 days of request. Note: If denial is for certain reasons (see AS-35 for explanation), individual can request in writing for decision to be reviewed by Patient Care Managers/IHS Coordinators who did not participate in the original decision to deny access. ADH must provide or deny access based on this determination.

If review is requested:

Contacts ADH Privacy Officer/Program Consultant, who contacts Patient Care Manager/IHS Coordinators for review of "reviewable" PHI to determine if PHI can be released.

Responsibility

ADH Patient Care Manager/IHS
Coordinators/ADH Privacy Officer/
Program Consultant

Action

Members who did not participate in
the original decision review request
and determine if PHI can be released.

Notifies Local Health Unit Administrator/
IHS Administrator of decision. If denied,
sends letter to requesting individual and a
copy to the Local Health Unit Administrator/
IHS Administrator. Note: Other information
is made accessible to the individual after
excluding the PHI that was denied access.

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO REQUEST AMENDMENT OF PROTECTED HEALTH INFORMATION

I. Policies:

(1) An individual has the right to request an amendment to his/her health information if he/she feels the information is incorrect or incomplete. ADH will review the request and grant or refuse the request. Requests for amendment of protected health information must be made in writing to the LHU Administrator of the Local Health Unit where the client's medical records reside and must clearly identify the information to be amended and the reasons for the amendment.

- (a) Request is Granted. If the individual responsible for the entry to be amended grants the request after review and approval, ADH must:
 - (a) Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment.
 - (b) Inform the individual that the amendment is accepted.
 - (c) Obtain the individual's identification of and agreement to have ADH notify the relevant persons with whom the amendment needs to be shared.
 - (d) Within a reasonable timeframe, make reasonable efforts to provide the amendment to persons identified by the individual, and persons, including business associates, that ADH knows have the protected health information that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the individual.
- (b) Request is Denied. Requests may be denied if the material requested to be amended:
 - (a) Was not made by ADH, unless the originator is no longer available to act on the request.
 - (b) Is not part of the individual's health record.
 - (c) Is not accessible to the individual because federal and state laws do not permit it (see reasons for denial of request to inspect or copy listed on AS-35).
 - (d) Is accurate and complete.

- (2) ADH must act on the individual's request for amendment no later than 60 days after receipt of the amendment. ADH may have a one-time extension of 30 days for processing the amendment if the individual is given a written statement of the reason for the delay and the date by which the amendment request will be processed.
- (3) If the request is denied, ADH must provide the individual with a timely written denial by issuing a Denial of Amendment Request (AS-36). The AS-36 must be written in plain language and must contain the following:
 - (1) The basis for the denial.
 - (2) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.
 - (3) A statement that if the individual does not submit a statement of disagreement, the individual may request that ADH provide the individual's request for amendment and the denial with any future disclosures of the protected health information that was the subject of the request.
 - (4) A description of how the individual may complain to ADH or the Secretary of Health and Human Services.
 - (5) The name or title and the telephone number of the designated contact person who handles complaints for ADH.
- (4) ADH must permit the individual to submit to ADH a written statement disagreeing with the denial of all or part of the requested amendment and the basis of such agreement. ADH may reasonably limit the length of a statement of disagreement.
- (5) ADH may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, ADH must provide a copy to the individual who submitted the statement of disagreement.
- (6) ADH must, as appropriate, identify the record of protected health information that is the subject of the disputed amendment and append or otherwise link the individual's request for amendment, ADH denial of the request, the individual's state of disagreement, if any, and ADH's rebuttal, if any.
- (7) If the individual has submitted the statement of disagreement, ADH must include the material appended or an accurate summary of such information with any subsequent disclosure of the protected health information to which the disagreement relates.

- (8) If the individual has not submitted a written statement of disagreement, ADH must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of protected health information only if the individual has requested such action.
- (9) When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, ADH must separately transmit the material required.
- (10) A covered entity that is informed by ADH of an amendment to an individual's protected health information must amend the protected health information in written or electronic form.
- (11) ADH must document the titles for the persons or offices responsible for receiving and processing requests for amendments.
- (12) Amendments received from other covered entities:
- (a) When a provider receives notification from another health care provider or health plan that a patient's protected health information has been amended, the receiving provider must:
- (1) Ensure that the amendment is appended to the patient's health record.
 - (2) Inform its business associates that may use or rely on the patient's protected health information of the amendment (as agreed to in the business associate contract), so that they may make the necessary revisions based on the amendment.

II. Procedures:

Responsibility

Action

Individual

Provides a written request to amend his/her protected health information to the Local Health Unit.

Notes: 1. The request must provide a reason to support the amendment.
2. The Agency must act on the request no later than 60 days after receipt of the request.

<u>Responsibility</u>	<u>Action</u>
LHU Administrator/IHS Administrator/Designee	Reviews record and sends request and copy of information to ADH Privacy Officer/ Program Consultant.
ADH Privacy Officer/Program Consultant	Informs the ADH Privacy/Security Officer and contacts Patient Care Horizontal Team/IHS Coordinators for determination of amendment.
ADH Patient Care Horizontal Team/ IHS Coordinators	Determines if amendment is accepted or denied.
	<u>If request for amendment is accepted:</u>
	Notifies the LHU Administrator/IHS Administrator, ADH Privacy Officer/Program Consultant, and ADH Privacy/Security Officer of determination.
LHU Administrator/IHS Administrator/Designee	In consultation with PHN/HHN, ensures individual's medical record is appropriately amended. Informs the individual that his/her record has been amended.
	Informs relevant persons that the individual's record has been amended if <u>requested by the individual</u> .
	<u>Notes:</u> 1. Relevant persons include: <ul style="list-style-type: none">-Persons identified by the individual as having received incorrect health information.-Business associates that have incorrect health information and may have relied on the information to the detriment of the individual.
	2. If informed by another covered entity of an amendment to health information, amend the medical record following these procedures.

Responsibility

Action

LHU Administrator/IHS
Administrator/Designee

If request for amendment is denied:

Completes and provides to the individual the Denial of Amendment Request (AS-36).

Permits the individual to submit a statement of disagreement with the AS-36.

Notifies ADH Privacy Officer/Program Consultant of statement of disagreement.

ADH Privacy Officer/Program
Consultant

Works with ADH Privacy/Security Officer and LHU Administrator/IHS Administrator to prepare rebuttal statement with advice from Legal Services to the individual's statement of disagreement.

LHU Administrator/IHS
Administrator

Places a copy of the rebuttal statement in the client's medical file and provides a copy to the client.

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO REQUEST CONFIDENTIAL COMMUNICATION

Policies:

- A. Individuals have the right to request that the Agency communicate with them about health care matters in a certain way or at a certain location, but must specify how or where they want to be contacted.
- B. ADH must permit clients to request and must accommodate reasonable requests by clients to receive communications of protected health information (PHI) from ADH by alternate means or at alternate locations. Examples of such requests may include, but are not limited to, mailing PHI to an alternate address specified by the individual, transmission of such information to a specific phone number by facsimile, transmission of such information via e-mail or a request that the Agency only contact the individual at work.
- C. The Department is not required to accommodate unreasonable requests for alternate delivery of PHI. Examples of such requests may include asking for delivery of PHI by registered or certified mail or requesting that PHI be hand carried to the client to an off-site location.
- D. The client must request in writing to receive PHI from ADH by alternate means or to an alternate location and must specify the preferred alternate means or location.
- E. Documented client requests for alternate means of delivery or alternate locations for delivery of PHI will be filed in the client's record and appropriate updates will be made to the client's record.
- F. Prior to sending any PHI to a client, ADH staff will review the client's record to confirm whether the client has requested that PHI be sent by alternate means or to an alternate location.
- G. ADH will forward PHI to the client in accord with the client's preferred means or location when requested or to his/her current mailing address, as appropriate.
- H. ADH may terminate its agreement to deliver PHI via alternate means or to an alternate location if:
 - (1) The client agrees to or requests termination of the alternate delivery location or method of communication in writing. ADH staff must document the request in the client's record.
 - (2) Use of the alternate delivery location or method of communication is not effective (i.e., ADH is unable to contact the client at the location or in the manner requested by the client). In this instance, ADH must inform the client that it is terminating its agreement to alternate means or location of delivery of PHI and provide the reason(s) for termination of the agreement.

- I. ADH must retain all documentation related to requests for alternative means of delivery of PHI or alternate delivery location for PHI for a minimum period of six years.
- J. When the client terminates the request for alternate delivery of PHI or it is determined that the alternate method of delivery is unreliable (i.e., mail has been returned, FAX machine number has been disconnected or has no FAX to receive messages, etc.), the ADH will notify:
 - A. The client of the termination of alternate delivery of PHI
 - B. The ADH Privacy Officer/Program Consultant

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO REQUEST RESTRICTIONS

I. Policies:

A. HIPAA requires ADH to permit an individual to request that ADH restrict health care information the Agency uses or releases for treatment, payment, operations, or disclosures permitted to family members, other relatives or close personal friends of the individual for involvement in the individual's care and notification purposes.

For example, a patient could request that his or her records not be shared with a particular physician because the physician is a family friend, or an individual could be seeking a second opinion and might not want his or her treating physician to be consulted.

B. HIPAA does not require ADH to agree or comply with the requested restriction or limitation. However, if ADH does agree to a restriction, it may not use or disclose PHI in violation of such restriction.

II. Procedures:

Responsibility

Action

Individual

Provides a written request for a restriction to the Local Health Unit.

Local Health Unit

Consults with PHN/HHN (if Local Health Administrator/IHS Unit Administrator is not a PHN/HHN) to Administrator/designee to determine if restriction is granted/denied.

Note: ADH must permit an individual to request restrictions on use/disclosure for treatment, payment, health care operations, involvement in individual's care, and notification purposes.
ADH is not required to agree to a restriction.

If restriction is denied:

LHU Administrator/IHS
Administrator/Designee

Documents request and denial in individual's chart.

Responsibility

Action

If restriction is granted:

LHU Administrator/IHS
Administrator/Designee

Documents restriction in individual's chart. Note: ADH may not use or disclose protected health information in violation of the restriction unless for emergency treatment. Then, ADH must request that emergency providers do not use or disclose further. Restrictions are not effective to prevent uses or disclosures when:

- required by law,
- for public health activities,
- about victims of abuse, neglect, or domestic violence,
- for health oversight activities,
- for judicial and administrative proceedings,
- for law enforcement purposes,
- about decedents,
- for cadaveric organ, eye or tissue donation purposes,
- for research purposes,
- to avert a serious threat to health or safety,
- for specialized government functions, and
- for workers' compensation.

Termination of a restriction:

Individual

Agrees to or requests termination of restriction in writing.

LHU Administrator/IHS
Administrator/Designee

Informs individual that the restriction will not apply to future protected health information created or received.

Covansys®
A CSC Company



Arkansas WIC Project

Operations Manual
June 13, 2008

ARKANSAS WIC OPERATIONS MANUAL

TABLE OF CONTENTS

1.0	GENERAL INFORMATION	2
1.1	System Overview	2
1.2	Identify Points of Contact	2
2.0	SYSTEM OPERATIONS OVERVIEW	3
2.1	System Operations.....	3
	Arkansas WIC Topology.....	4
2.2	Prepare a Hardware Inventory.....	5
2.3	Prepare a Software and Operating System Inventory.....	7
2.4	Prepare a Processing Overview.....	7
2.5	Prepare a Communications Overview	7
2.6	Account Creation.....	8
2.7	Updating Vendor Letters	14
2.8	Updating Other Mail-Merge Documents	18
2.9	Establish a Maintenance and Backup Schedule	19
2.10	Establish Guidelines for System Shutdown and Recovery.....	21
2.11	Establish Guidelines for Environment and Security.....	28
3.0	SITE OPERATIONS OVERVIEW	36
3.1	Document Maintenance Best Practices.....	36
3.2	Document Communication Requirements.....	36
3.3	Document Troubleshooting FAQ.....	37
4.0	Appendices	40
	APPENDIX A – INSTALLATION INSTRUCTIONS	41
	Installation Instructions	41
	APPENDIX B – DISASTER RECOVERY PLAN	63
	APPENDIX C – GLOSSARY OF TERMS	69
	APPENDIX D – END OF MONTH (SYSTEM ADMINISTRATION)	78
	APPENDIX E – END OF DAY (SYSTEM ADMINISTRATION)	89
	APPENDIX F – ON-GOING MAINTENANCE, REPAIR AND REPLACEMENT OF ARKANSAS AGENCY EQUIPMENT	105
	APPENDIX G – SETUP PROCEDURES FOR DATA SYNC	106

1.0 GENERAL INFORMATION

1.1 System Overview

Arkansas WIC is an automation system for the Supplemental Nutrition Program for Women, Infants, and Children (WIC Program). This is an on-line, web-based system with a central host that will support clinic and state office functions. The Arkansas WIC application will automate a number of functions at both the local service delivery sites and the Arkansas WIC state office.

1.2 Identify Points of Contact

During the installation set-up phase of implementation and also after the system is in operation, it will be helpful to have contact lists at hand to aid in timely response to questions and problems.

1.2.1 Coordination

The Arkansas WIC Information Technology group will supply a list of organizations that require coordination between the project and its specific support functions, e.g., installation coordination and security will be provided by Arkansas WIC MIS Staff.

1.2.2 Help Desk

Helpdesk information, including responsible personnel phone numbers for emergency assistance, will be provided by Arkansas WIC MIS Staff.

1.2.3 Clinic Personnel

The Arkansas WIC state office will be responsible for providing a list of clinic personnel to be contacted during the installation of equipment and software for their specific location. This same list of personnel can be used after implementation to effectively respond to problems and questions.

1.2.4 State Office Personnel

The Arkansas WIC state office will be responsible for providing a list of state office personnel to be contacted during the installation of equipment and software at the state office.

2.0 SYSTEM OPERATIONS OVERVIEW

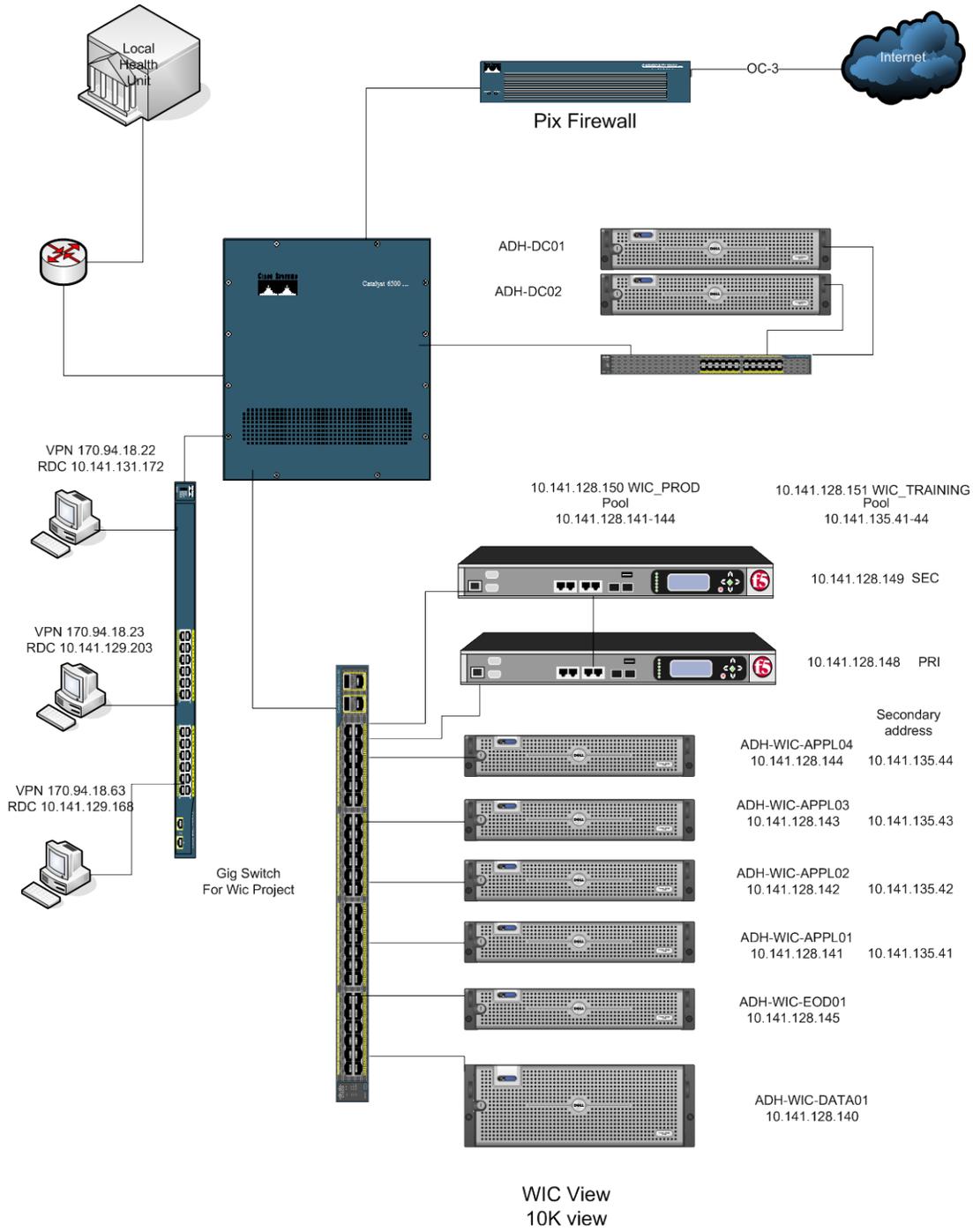
2.1 System Operations

A significant amount of initial planning occurs to ready a system such as the Arkansas WIC application for day-to-day operational activity. Initially, inventories are taken of hardware, software and operating systems so each site can be prepared to function in a production environment.

- This plan does not include the detailed list of hardware.
- This plan does not include the detailed list of software and operating systems loaded on each type of production machine.
- This plan does not include the operational inventory.

All of these lists will be provided by Arkansas WIC Information Technology along with or as part of the site surveys.

Arkansas WIC Topology



2.2 Prepare a Hardware Inventory

The Arkansas WIC Information Technology group will provide a complete hardware inventory based on the site surveys collected for each site. The list will contain item model number, any other identifying information and the quantity on hand for all hardware to be used for the WIC system implementation:

- Servers
- Storage Devices
- Operating System for DNS Servers
- Backup Software and Tapes
- Firewall Bundle
- Network Switches
- Additional equipment, if any

Below is a sample table showing the types of information to be gathered. Note that the information in the table is not specific to Arkansas WIC, but is shown only as an example of the type of information to be collected.

Arkansas Department of Health IT to fill this table out:

<u>Web Server-PowerEdge 2950 III</u>	<u>4</u>
Dual Core Intel Xeon X5260, 6MB Cache, 3.33GHz, 1333MHz FSB, Windows Server 2003 R2, Standard Edition with SP2	1
Dual Embedded Broadcom NetXtreme II 5708 Gigabit Ethernet NIC	1
4GB 667 MHz (4x1GB), dual Ranked DIMMS	1
146GB 15K RPM Serial-Attached SCSI 3Gbps 3.5-in HotPlug Hard Drive	2
Integrated SAS/SATA RAID 1, PERC 6/I Integrated/SAS6/iR	1
Energy Smart Redundant Power Supply with Y-Cord	1
Rack Chassis w/Sliding Rapid/Versa Rails and Cable Management Arm, Universal	1
<u>EOD Server-PowerEdge 2950 III</u>	1
Dual Core Intel Xeon X5260, 6MB Cache, 3.33GHz, 1333MHz FSB, Windows Server 2003 R2, Standard Edition with SP2	1
Dual Embedded Broadcom NetXtreme II 5708 Gigabit Ethernet NIC	1
4GB 667 MHz (4x1GB), dual Ranked DIMMS	2
146GB 15K RPM Serial-Attached SCSI 3Gbps 3.5-in HotPlug Hard Drive	2
Integrated SAS/SATA RAID 1, PERC 6/I Integrated/SAS6/iR	1
Energy Smart Redundant Power Supply with Y-Cord	1
<u>PROD SQL DB SERVER</u>	1
2x Quadl core Intel Xeon Processor, Windows Server 2003 R2, 32 Bit-Enterprise Edition with SP2	1
SQL 2000 Server	1

Dual Embedded Broadcom NetXtreme II 5708 Gigabit Ethernet NIC	1
16GB Memory, 8x2GB, 667MHz, Dual Ranked DIMMS	1
300GB 15K RPM Serial-Attach SCSI 3Gbps 3.5-in HotPlug Hard Drive – 3ea RAID 5, 1ea Hot Swap Drive	4
PERC 5i RAID Controller, 3 to 5 Hard Drives in RAID 5 config	1
1x5 SAS Backplane, 3.5 Inch SAS Hard Drives	1
PERC 5/I SAS RAID Controller, Internal, PCIe	1
QLogic QLE2460 Fibre Channel HBA, Single Channel, 4Gb, Optical, PCIe	2
Dell Versa Rails for use in Third Party Rack, Round Hole	1

Item/Details	Quantity
<u>Operating System for DNS Servers</u>	
Solaris 9 1-2 CPU RTU License for Intel Platform	2
2.0	3.0
<u>Backup Software and Tapes</u>	
Symantec Backup Exec 11d for Windows Server	1
4.0	5.0
<u>Firewall Bundle</u>	
PIX 525-FO-GE Bundle (Chassis, Failover SW,2 GE+2 FE,VAC+)	1
Power Cord,110V	1
PIX 525/535 3DES/AES VPN/SSH/SSL encryption license	1
PIX v6.3 Software for the 515E, 525 and 535 Chassis	1
PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+)	1
Cisco VPN Client Software (Windows, Linux, Solaris)	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
6.0	7.0
<u>Network Switches</u>	
24 10/100 ports w/2 1000BASE-SX ports, Standard Image only	2
Power Cord,110V	2
8x5xNBD Svc, 24 10/100 ports w/2 1000BASE-SX ports, S	2
1000BASE-SX Short Wavelength GBIC (Multimode only)	4
8.0	9.0

2.3 Prepare a Software and Operating System Inventory

Arkansas WIC Information Technology will provide an inventory list of all software that will be loaded on each type of machine used in the clinics and state office to access the Arkansas WIC application. The list will include software and operating system components for workstations and servers in the following groups:

- Client Desktop Workstations
- Client Laptop Workstations (if utilized)

2.4 Prepare a Processing Overview

Arkansas WIC Information Technology will prepare a processing overview to be included in the Operations Manual. The overview should include a list of servers and their specific function as related to the Arkansas WIC application.

2.5 Prepare a Communications Overview

The communications overview should include a description of the web and database servers, the application server that runs end-of-day and end-of-month batch processing and the database servers. It should include a description of communication between web servers and remote systems for both permanent connect remote locations and non-permanent connected remote locations. Arkansas WIC Information Technology is responsible for providing input for this task.

2.6 Account Creation

The following is a step by step guide for user account creation within the SPIRIT application.

2.6.1 Users

The **User Profile** screen is used to manage a user profile record and can be displayed in Add or View mode.

The screenshot shows a window titled "User Profile for [New User]". It contains several input fields and a table. The fields are: "User ID" (value: 123456), "First Name" (value: DOROTHY), "Middle Initial" (value: M), and "Last Name" (value: JONES). To the right of these fields is a section titled "Participant List Default View" with four radio buttons: "On-site" (selected), "Local", "Statewide", and "Appointments for Today". Below this is a "Status" section with a checked "Active" checkbox and an "Inactive Date" dropdown menu. Underneath is a "Staffing Assignments" section with an empty table. At the bottom of the window are buttons for "Add", "Edit", "Delete", "Set Password", "OK", and "Cancel".

User Profile Screen

To access this screen: Display the **WIC Management Console** screen in Security (Users) mode, and then do one of the following:

- To add a new user profile: On the **Users** menu, click **Add**.
- To view the details of a user profile: Select a user profile in the table > On the **Users** menu, click **View**.

2.6.2 Screen Elements:

User ID – Enter the staff member's user identification.

First Name – Enter the staff member's first name.

Last Name – Enter the staff member's last name.

Middle Initial – Enter the staff member's middle initial.

Participant List Default View – Select one of the radio buttons to indicate which view of the **Participant List** screen to display by default whenever the staff member first launches the application.

Active – Select this check box to indicate the staff member is currently active and able to access the application.

Inactive Date – Enter or select the date on which the staff member's user profile becomes inactive.

Staffing Assignments – View the current staffing assignments for the staff member in the table.

The following buttons are associated with the table:

- **Add** – Click this button to add an assignment to the **Staffing Assignments** table.
- **Edit** – Click this button to edit an assignment selected in the **Staffing Assignments** table.
- **Delete** – Click this button to delete an assignment selected in the **Staffing Assignments** table.

Set Password – Click this button to set the staff member's password.

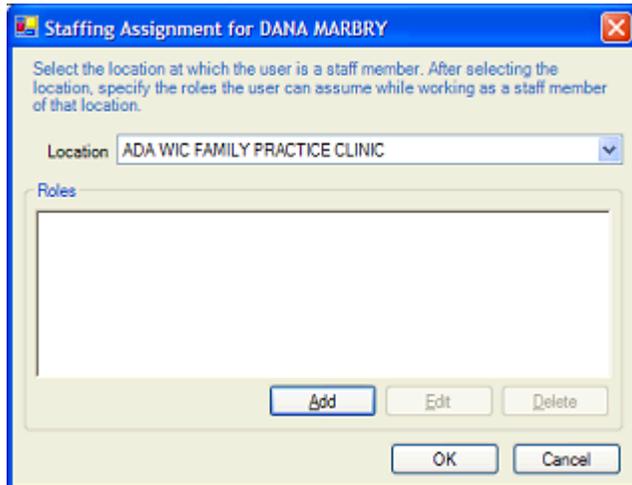
OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.6.4 Assignments, Passwords, and Roles

Staffing Assignment

The **Staffing Assignment** screen is used to manage the staffing assignments for a user profile record and can be displayed in Add or Edit mode.



Staffing Assignment Screen

To access this screen: Display the **User Profile** screen, and then do one of the following:

- To add a new staffing assignment: Click **Add**.
- To edit a staffing assignment: Select an assignment in the **Staffing Assignments** table > Click **Edit**.

2.6.5 Screen Elements:

Location – Select the location at which the staff member has an assignment.

Roles – View the current roles assigned for the staff member in the table. The following buttons are associated with the table:

- **Add** – Click this button to add a role to the **Roles** table.
- **Edit** – Click this button to edit a role selected in the **Roles** table.
- **Delete** – Click this button to delete a role selected in the **Roles** table.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.6.6 Set Password

The **Set Password** screen is used to manage password information.



Set Password Screen

To access this screen: Display the **User Profile** screen > Click **Set Password**.

2.6.7 Screen Elements:

Current Password – Enter the current password.

New Password – Enter the new password.

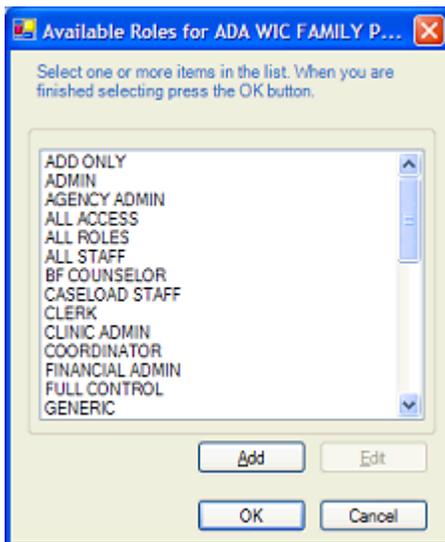
Confirm New Password – Enter the new password again for verification purposes.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

Select Roles

The **Select Roles** screen is used to select a specific role when creating a new staffing assignment.



Select Roles Screen

To access this screen:

Display the **Staffing Assignment** screen > Click **Add**.

2.6.8 Screen Elements:

Available Roles – Select a specific role to assign. The following buttons are associated with the table:

- **Add** – Click this button to add a role to the **Available Roles** table.
- **Edit** – Click this button to edit a role selected in the **Available Roles** table.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.6.9 Roles

The **Role Profile** screen is used to manage a role record and can be displayed in Add or View mode.

Feature Group	Feature	Access
Financial Management	Accounting Schedule	None
Financial Management	Financial Account Inqui	None
Financial Management	Financial Accounts	None
Financial Management	Financial Management	None
Financial Management	Financial Reports	None
Financial Management	Financial Statements	None

Role Profile Screen

To access this screen:

- To add a new role: Display the **WIC Management Console** screen in Security (Roles) mode > On the **Roles** menu, click **Add**.
- To view the details of a role: Display the **WIC Management Console** screen in Security (Roles) mode > Select a role in the table > On the **Roles** menu, click **View**.
- To add a new role while working with a user profile: Display the **Select Roles** screen > Click **Add**.
- To edit a role while working with a user profile: Display the **Select Roles** screen > Select the role to edit > Click **Edit**.

2.6.10 Screen Elements:

Role Name – Enter the name of the role.

Description – Enter a brief description of the role.

Permissions – A list of all available permissions are displayed in the table. Select the **Access Level** per permission by clicking directly in the column. The following button is associated with the table:

- **Reset** – Click this button to reset the list of permissions currently displayed in the **Permissions** table to their initial settings.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.7 Updating Vendor Letters

Please Note: Text in the letter template that is in << >> brackets are the mail merge value(s) and can never be deleted or modified without program changes. Modifying these fields will cause errors in the Mail Merge process.

Microsoft Word is required to update the Vendor Letters.

Vendor Letters are stored in the **c:\Program Files\Covansys Inc. - BPDS\WIC\Templates** directory.

Before you begin working, copy all letters to a different working directory on your hard drive for modifying. When modifications are completed, copy the modified letters to the Templates directory (listed above) and test them by printing from the Vendor Management Application. Additional modifications can be made as needed. The letter templates are written in Microsoft Word template using a mail merge. **Text in the letter template that is in << >> brackets is the mail merge value(s) and can never be deleted or modified without program changes.**

It is also very important to keep all Vendor Letters backed up to a CD or a backup directory on the server.

SPIRIT Vendor Form Letters

Letter Title	File Name
Applications	
Vendor Application	AP001
Vendor Application - Chain/Commissary	AP002
Vendor Application – Pharmacy	AP003
Vendor Application - Pharmacy Chain	AP004
Vendor Waiting List	AP005
Interim Application Letter	AP006
Application Approval	AP007
Application Denial	AP008
Expiration of Contract	AP009
Checks/Compliance Buys	
WIC Checks Submitted for Replacement - Redeposit	CH020
WIC Checks Submitted for Replacement - Not Replaced	CH021
Compliance Buy	CH022
Compliance Buy Meeting Letter	CH023
WIC Checks Submitted for Replacement - Redeposit	CH025
Disqualification	
Contract Termination - Store Closing	DQ040
Contract Termination - Change in Ownership	DQ041
Contract Termination - Withdrawal from Program	DQ042
Notification to Food Stamps of WIC Disqualification	DQ043
Disqualification Notification - Final Notice	DQ045
Monitoring	
Vendor Monitoring Visit	MN060
Onsite Warning	MN061

Notification General Information	
CPL Notification - CPL Survey	NG080
Stamps	
Vendor New Stamp	ST100
Vendor Replacement Stamp	ST101
Fee for Replacement of Lost Stamp	ST102
Training	
Annual Vendor Training	TR120
Special Training	TR122
Orientation Training	TR123
Vendor Training for All New Vendors	TR124
Make-up Vendor Training for New Vendors	TR125
Interactive Training	TR126
Vendor Price Survey	TR127

We will use letter AP001.DOC and CH020.DOC as examples. The remainder of the letters should be modified using the same practices.

To Begin Updating:

Double click on a letter to modify in your WORKING directory.

Example: Create directory C:\UPDATED VENDOR LETTERS on your local machine.

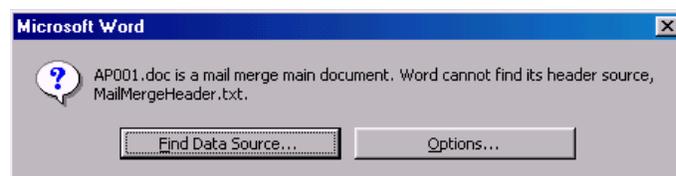
Copy all letter templates from C:\Program Files\Covansys Inc. -

BPDS\WIC\Templates to C:\UPDATED VENDOR LETTERS. Double click on any letter.

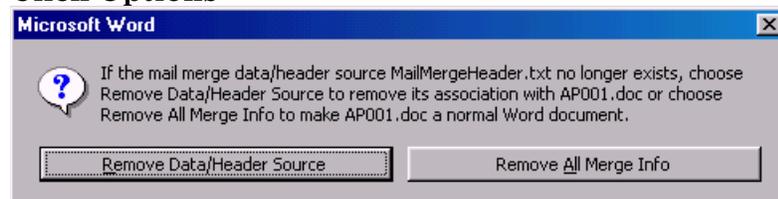
For this exercise, AP001.DOC is selected.

Note:

If you see this message



Click Options



Click Remove all Merge Info

The document will open in Microsoft Word.

You can now update this letter as you would any Microsoft word document.

It is important to leave all mail merge information intact.

Example 1:

In Letter AP001.DOC, the Header information can be deleted and replaced with any information you want to appear on your letterhead.



Arkansas Department of Health

ADDRESS ONE
CITY, STATE ZIP

STATE GOVERNOR
Governor

STATE COMMISSIONER
Commissioner

Just below the Header in the body of the document you will find the following information:

«LetterDate»

«Salutation» «FirstName» «LastName», «Title»

«Vendor»

«AddressLine1»

«AddressLine2»

«City», «ST» «ZIPCode»

SUBJECT: Vendor Application - Due Date Postmarked by April 15, 2000

Dear «Salutation» «LastName»:

The State Supplemental Nutrition Program for WIC is now accepting applications from retail food stores and pharmacies ...

The Subject line and the body of the letter can be changed. The bottom of this and all letters also include a mail merge value for <<userid>> to indicate who generated the letter. If this or any mail merge value is deleted, you may encounter errors when printing the letter.

Example 2:

Open the letter template CH020.DOC. This letter has mail merge values gathered in the body of the letter to include check numbers and issue dates for check that have been approved and require redeposit.

<u>Check Number</u>	<u>Issue date</u>
«ReturnedCheck1»	«IssueDate1»
«ReturnedCheck2»	«IssueDate2»
«ReturnedCheck3»	«IssueDate3»
«ReturnedCheck4»	«IssueDate4»
«ReturnedCheck5»	«IssueDate5»

In this letter you can change the text that is surrounding these mail merge values. Do not change any value within the <<>> brackets.

Move the letters to Templates folder:

Once you have completed updating the first letter, test it from the Vendor Management system. Copy the letter to the **C:\Program Files\Covansys Inc. - BPDS\WIC\Templates** directory.

To test printing letter AP001.DOC from the Vendor application, open a Vendor folder for a Vendor who is independently owned. Click the Event Log tab of the Vendor Folder. Highlight the Applicant event in the Events tree view. Click the Details button. Click Send Application. Select a recipient and a mailing address. Click OK.

Review the letter and make additional modifications as necessary.

2.8 Updating Other Mail-Merge Documents

In addition to vendor letters, there are some additional letter and form templates that are set up as Microsoft Mail-Merge documents. Participant specific information is merged into these letters or documents as they are printed. Arkansas WIC will be responsible for updating the basic content of each letter and form tailoring the wording and Arkansas specific information for the Arkansas WIC application.

Letter Title	File Name
English - Appointment Notice (Letter)	AN001
English - Appointment Notice (Postcard)	AN002
Spanish - Appointment Notice (Letter)	AN003
Spanish - Appointment Notice (Postcard)	AN004
English - Missed Appointment Notice (Letter)	MAN001
English - Missed Appointment Notice (Postcard)	MAN002
Spanish - Missed Appointment Notice (Letter)	MAN003
Spanish - Missed Appointment Notice (Postcard)	MAN004
English – Official Notice (Letter)	ON001
English – Official Notice (Postcard)	ON002
Spanish – Official Notice (Letter)	ON003
Spanish – Official Notice (Postcard)	ON004
Prescription Formula Request Form	PrescriptionFormulaRequestReport

2.9 Establish a Maintenance and Backup Schedule

This task establishes a routine maintenance and backup schedule for production servers. The Operations Manual contains recommendations for monthly server maintenance, a server backup schedule and retention times for the server backups. ADH IT will be responsible for the final maintenance and backup schedules and retention cycle. Also included in the Operations Manual is a recommended database backup schedule including daily, weekly, and monthly backups.

Recommended Monthly Server Maintenance:

CSC Covansys recommends ADH IT performs monthly server maintenance to install security patches and hot fixes, reboot systems, test fail-over and clean disk space. In case of emergency updates, the IT team should contact all effected personnel with time of expected updates to schedule a time for the updates with minimal production outage.

Recommended Server Backup Schedule:

The following is a recommended schedule of start times and duration of backup schedules:

- Incremental backups should run daily Monday -Thursday evening.
- Full Backups should run each Friday evening.
- The 2nd Saturday of every month should be designated the Month-End Full backup.
- After completing Month-End processing for September, the 2nd Saturday of October should be designated the Year End Full backup.
- All backup tapes should be taken off-site daily to a secure facility.

Recommended retention times:

Dailies: 2 weeks

Full: 2 weeks

Month End: 1 year

Year End: Infinite

Recommended Database Backup Schedule:

Daily Database Server Maintenance

- Full database export backups of both database structure without data and database structure with data (Monday-Saturday).
- Full database hot backup (Monday-Saturday).
- Generate a script that will create the database with current structure.
- Update statistics on production schema objects (Monday-Friday).
- Every 15 minutes run a script that checks to see if database instance is up and page the on call DBA if it is down.
- Every 15 minutes run a series of database monitoring scripts and page the on call DBA if specific thresholds are exceeded.
- Every 30 minutes gather operating system performance metrics that can be used to troubleshoot database performance issues.
- Run SQL Server reports hourly to gather database performance metrics (Monday-Friday).
- Run a series of general database health monitoring scripts and email the results to the DBA group.
- Extract any SQL Server errors out of database alert log and email them to DBA team.

Weekly Database Server Maintenance

- A cold database backup should be performed every Sunday night.
- Compress database listener log and start new one during cold backup.
- Delete old logs and trace files.

Monthly Database Server Maintenance

- Compress database alert log and begin new one on the first day of each month.
- Reorganize any needed database objects.
- Apply any database patches as needed.

2.10 Establish Guidelines for System Shutdown and Recovery

Arkansas Department of Health IT will fill in this information based on the server setup. The information in this section is a sample representation of the System Shutdown and Recovery procedures.

Individual Server Reboot:

5 servers can be rebooted at any time if no user is on the system.

- 1) Application Server (EOM/EOD)
- 2) Testing Box (1)
- 3) Testing Box (2)
- 4) FTP server
- 5) DNS Server

4 servers are load balanced so you would reboot one completely then the other.

- 1) Domain Controller01
- 2) Domain Controller02
- 3) WebServer01
- 4) WebServer02

2 Servers are clustered. Database01 is currently being used so if a total reboot is needed, it would be Database02. After it's completely up Database01 can be rebooted and the cluster.

- 1) Database01 - Database Server (1) will be set to fail over.
- 2) Database02 - Database Server (2) will be set to fail over.

The Application server can be rebooted at any time as long as it is up and running before the EOM process or EOD process is to start running. **Do not** reboot this server during the EOM or EOD process.

The Raid Array **should not** have to be rebooted. If power or connection is lost, this would bring the entire system down. All data is stored in the Raid Array.

The FTP Server **should not** be rebooted during a transfer. If files were being transferred and the server is rebooted, the file **will not** be automatically resent.

The Database Servers should be set to fail over. If one Database Server was shut off, the end users should not notice anything. If both Database boxes lost power or connection at the same time this would bring the entire system down.

The test servers **do not** need to be rebooted.

If there is a planned update to the Data or Applications servers (Web/Application), reboot both DB servers and then reboot both Web servers. This process should be done after hours or with the knowledge that all users will be kicked off the system.

Entire System Shutdown:

1. If all servers need to go offline, you will want to do so in the following order:
2. Shutdown the web cluster servers first. You will want to bring one server down at a time. Wait until the servers are offline to ensure users don't have an active connection.
3. Shutdown the Application Server (EOD/EOM)
4. Shut down the MSSQL Server Cluster. You will want to turn off SERVER-X first, then turn off SERVER-Y
5. Shut down the Active Directory Servers

Entire System Startup:

1. The Active Directory servers should be started first.
2. After the AD servers are online, Turn on the MSSQL Servers and wait for each individual server to start before bringing the next server online.
3. Start the Application Server (EOD/EOM)
4. Turn on Web Servers one at a time; wait for each individual server to start before bringing the next server online.

Clustered Servers Troubleshooting:

Server Clusters: Backup and Recovery Best Practices for Windows Server 2003

Published: January 1, 2003

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/clustering/sercbrbp.mspx>

There are potentially two kinds of backups for Microsoft Windows Server 2003: An Authoritative System Restore (ASR) backup including the cluster configuration (we will refer to this as System State Backup) or a backup that is purely local (we will refer to this as a Local Backup). Note that to perform an Authoritative Restore, a System State Backup is required. If you perform an Authoritative Restore on one node, Microsoft recommends that you do a Non-Authoritative Restore on the other cluster nodes.

Cluster nodes fail to boot

In this case we assume that the quorum disk is functional and all of the data is intact.

One node in the cluster fails to boot

The other nodes in the cluster are running as expected.

Recommendation

Use Non-Authoritative Restore. This should work with either System State Backup or a local Backup.

This will result in the cluster database on the damaged node being restored and then the affected node should be able to re-join the cluster. In this case, it will download the most recent copy of the cluster database from the other nodes in the cluster.

All nodes in the cluster fail to boot

None of the cluster nodes are able to boot.

Recommendation

Use Non-Authoritative Restore on one node. Assuming the quorum disk is fine, the node should be able to form the cluster with the state on the quorum disk. If that does not work, then try the Authoritative Restore (this needs System State Backup) on the node.

Use Non-Authoritative Restore for all of the other nodes.

All nodes are fine but the quorum disk is not functional

The cluster nodes boot, but the cluster service cannot start on any of the nodes because it cannot bring the quorum resource online. An entry in the eventlog should point to the inability to bring the quorum online.

Recommendations

Replace the quorum disk if the drive itself has failed or reformat the quorum disk if the physical drive has not failed. Use an Authoritative Restore, if you have one, to bring up one node.

OR

Use the fixquorum flag to start the cluster service (note that fixquorum allows you to start the cluster service with a broken quorum resource that fails to come online but does not really fix any data for you) and chose an alternate quorum resource (local quorum can be used if you do not have another disk). By setting a new quorum, new quorum log files are created on the quorum but the registry checkpoint files are not restored because the old quorum is not available.

A Reskit tool ClusterRecovery is available to help with this procedure.

Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint files.

Cluster database corruption on one of the Cluster Nodes

You can discover that this is the case if the node does not join and the entries in the cluster log (found at %windir%\cluster\cluster.log by default) point to a corrupted hive.

Recommendations

Do a Non-Authoritative Restore on this node and have it join the cluster

OR

Copy the latest checkpoint (chkXXX.tmp) file from the quorum disk and overwrite the file %windir%\cluster\clusdb on the affected node and restart the service.

OR

Stop the service on a working cluster node. Unload the cluster hive using RegEdit.

Copy the file %windir%\cluster\clusdb from the working node to %windir%\cluster\clusdb on the affected node, and restart the cluster service on all nodes.

All nodes were running fine but the quorum database became corrupt

In this case, no node is able to form the cluster and an entry in the eventlog points to a corrupt quorum log as the problem.

Recommendation

Start the cluster service with the resetquorumlogfile switch. If all of the resources start successfully and the configuration looks satisfactory then no action is required. By resetting the quorum, new quorum log files are created on the quorum disk but the registry checkpoint files are not restored because the old quorum is not available.

Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint files.

If that fails, use Authoritative Restore on one node and restart the cluster service to form the cluster. Use Non-Authoritative Restore on other nodes.

Checkpoint files are lost or corrupt

If a registry checkpoint file is not found or cannot be loaded because it has been corrupted, resources may not have the most up-to-date information in the registry when they are brought online. The impact depends on the resource, however, in some cases; the resource

may fail to come on line. In other cases, configuration changes that were made may be lost. If a checkpoint file is missing, the cluster service does not add an event to the event log, you will need to look at the cluster log if you suspect this is an issue.

Recommendation

If the resources fail to come online, use the resource kit tool ClusterRecovery to re-create the resource checkpoints.

Note: You should only restore the checkpoint files for resources that fail to come online.

If that does not solve the problem use Authoritative Restore on a cluster node and restart the cluster service to form the cluster. Use Non-Authoritative Restore on other nodes.

A cluster disk is corrupt or non functional

Resources that depend on this disk may not come online. The disk does not come online or the data on the disk is corrupt. There are two cases, either the disk needs to be replaced or it does not.

Disk itself is not corrupt and comes online

Recommendation

Restore the data to the disk

Disk is corrupt

Recommendations

Replace the disk and use a Non-Authoritative Restore on one node. Restore the data to the disk.

OR

Use the resource kit which contains a tool called ClusterRecovery which allows an existing physical disk resource to be replaced with a new disk without having to do a system state restore. Once the physical disk is brought online, you can restore any data.

Recovery without Backup of the System

In this case, we recommend procedures for troubleshooting some disaster scenarios without the use of a backup. The solution, for obvious reasons, may not be complete for all scenarios. Single System Corruption of one or more Cluster Nodes

In this case, we assume that the quorum disk is functional and the data is intact.

One node in the cluster fails to boot the other cluster nodes are running as expected.

Recommendation

Evict that node and try to find a replacement.

Join the new node to the cluster.

All nodes in the cluster are dead

Recommendation

You will have to rebuild the cluster from scratch.

All nodes are fine but the quorum disk is not functional

Recommendation

Use the fixquorum flag to start the cluster service (note that fixquorum allows you to start the cluster service with a broken quorum resource that fails to come online but does not really fix any data for you) and chose an alternate quorum resource (local quorum can be used if you do not have another disk). By setting a new quorum, new quorum log files are created on the quorum but the registry checkpoint files are not restored because the old quorum is not available.

A Reskit tool ClusterRecovery is available to help with this procedure. Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint issue.

The cluster database is corrupt on one of the Cluster Nodes

Recommendation

Copy the latest checkpoint (chkXXX.tmp) file from the quorum disk and overwrite the file %windir%\cluster\clusdb on the affected node and restart the cluster service.

OR

Stop the service on another node. Unload the cluster hive using RegEdit.

Copy the file %windir%\cluster\clusdb from one of running nodes in the cluster to %windir%\cluster\clusdb on the affected node and restart the cluster service on all nodes.

All nodes were running fine but the quorum database became corrupt

Recommendation

Start the cluster service with the resetquorumlogfile switch. If all of the resources start successfully and configuration looks satisfactory then no action is required. By resetting the quorum, new quorum log files are created on the quorum disk but the registry checkpoint files are not restored because the old quorum is not available.

Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint files.

Checkpoint files are lost or corrupt

If a registry checkpoint file is not found or cannot be loaded because it has been corrupted, resources may not have the most up-to-date information in the registry when they are brought online. The impact depends on the resource, however, in some cases; the resource may fail to come on line. In other cases, configuration changes that were made may be lost. If a checkpoint file is missing, the cluster service does not add an event to the event log, you will need to look at the cluster log if you suspect this is an issue.

Recommendation

If the resources fail to come online, use the resource kit tool ClusterRecovery to re-create the resource checkpoints.

Note: You should only restore the checkpoint files for resources that fail to come online.

A cluster disk is corrupt or non functional

Recommendation

If the disk has been forcefully dismounted, it may require chkdsk to run in order to bring the disk online. The cluster service will run chkdsk automatically when the disk is brought online. In Windows Server 2003, a chkdsk log is preserved so that you can see what state the disk is in and what issues were found. If the application data on the disk is corrupted or deleted and you do not have a backup, there is no way to recover the data. You will have to regenerate the data or re-build the application. Server clusters does not provide user data protection and redundancy, you should use redundant hardware (mirrored disks or RAID disks) and take frequent backups of the data.

2.11 Establish Guidelines for Environment and Security

We highly recommend a secure environment for servers and networking components, as well as a security policy for application access. Servers can be physically secured with the use of a lock system that requires security cards or biometric access

The optimum range for users that need to work in the server room, and equipment reliability, is normally between 68 to 74 degrees Fahrenheit. Aim to avoid temperature changes greater than 10 degrees F per hour and humidity changes of + or -10% in the same period. A relative humidity level between 45% and 60% are best for safe server operation and minimizes risk from static electricity.

Network Security Policy: Best Practices White Paper

<http://www.cisco.com/warp/public/126/secpol.html#t1>

Introduction

Without a security policy, the availability of your network can be compromised. The policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy and adapts to lessons learned.

This document is divided into three areas: preparation, prevention, and response. Let's look at each of these steps in detail.

Preparation

Prior to implementing a security policy, you must do the following:

- Create usage policy statements.
- Conduct a risk analysis.
- Establish a security team structure.

Create Usage Policy Statements

CSC Covansys recommends creating usage policy statements that outline users' roles and responsibilities with regard to security. You can start with a general policy that covers all network systems and data within your State or program. This document should provide the general user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If your State or program has identified specific actions that could result in punitive or disciplinary actions against an employee, these actions and how to avoid them should be clearly articulated in this document.

The next step is to create a partner acceptable use statement to provide partners with an understanding of the information that is available to them, the expected disposition of that information, as well as the conduct of the employees of your company. You should clearly explain any specific acts that have been identified as security attacks and the punitive actions that will be taken should a security attack be detected.

Lastly, create an administrator acceptable use statement to explain the procedures for user account administration, policy enforcement, and privilege review. If your State or program has specific policies concerning user passwords or subsequent handling of data, clearly present those policies as well. Check the policy against the partner acceptable use and the user acceptable use policy statements to ensure uniformity. Make sure that administrator requirements listed in the acceptable use policy are reflected in training plans and performance evaluations.

Conduct a Risk Analysis

A risk analysis should identify the risks to your network, network resources, and data. This doesn't mean you should identify every possible entry point to the network, nor every possible means of attack. The intent of a risk analysis is to identify portions of your network, assign a threat rating to each portion, and apply an appropriate level of security. This helps maintain a workable balance between security and required network access.

Assign each network resource one of the following three risk levels:

- Low Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.
- Medium Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.
- High Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Assign a risk level to each of the following: core network devices, distribution network devices, access network devices, network monitoring devices (SNMP monitors and RMON probes), network security devices (RADIUS and TACACS), e-mail systems, network file servers, network print servers, network application servers (DNS and DHCP), data application servers (SQL Server or other standalone applications), desktop computers, and other devices (standalone print servers and network fax machines).

Network equipment such as switches, routers, DNS servers, and DHCP servers can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. Such a failure can be extremely disruptive to the business.

Once you've assigned a risk level, it's necessary to identify the types of users of that system. The five most common types of users are:

- Administrator's internal users responsible for network resources.
- Privileged internal users with a need for greater access.
- Internal users with general access.
- Partners External users with a need to access some resources.
- Others External users or customers.

The identification of the risk level and the type of access required of each network system forms the basis of the following security matrix. The security matrix provides a quick

reference for each system and a starting point for further security measures, such as creating an appropriate strategy for restricting access to network resources.

System	Description	Risk Level	Types of Users
ATM switches	Core network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Network routers	Distribution network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Closet switches	Access network device	Medium	Administrators for device configuration (support staff only); All others for use as a transport
ISDN or dial up servers	Access network device	Medium	Administrators for device configuration (support staff only); Partners and privileged users for special access
Firewall	Access network device	High	Administrators for device configuration (support staff only); All others for use as a transport
DNS and DHCP servers	Network applications	Medium	Administrators for configuration; General and privileged users for use
External e-mail server	Network application	Low	Administrators for configuration; All others for mail transport between the Internet and the internal mail server
Internal e-mail server	Network application	Medium	Administrators for configuration; All other internal users for use
SQL Server database	Network application	Medium or High	Administrators for system administration; Privileged users for data updates; General users for data access; All others for partial data access

Establish a Security Team Structure

Create a cross-functional security team led by a Security Manager with participants from each of your operational areas. The representatives on the team should be aware of the security policy and the technical aspects of security design and implementation. Often, this requires additional training for the team members. The security team has three areas of responsibilities: policy development, practice, and response.

Policy development is focused on establishing and reviewing security policies for the company. At a minimum, review both the risk analysis and the security policy on an annual basis.

Practice is the stage during which the security team conducts the risk analysis, the approval of security change requests, reviews security alerts from both vendors and the CERT leavingcisco.com CERT mailing list, and turns plain language security policy requirements into specific technical implementations.

The last area of responsibility is response. While network monitoring often identifies a security violation, it is the security team members who do the actual troubleshooting and fixing of such a violation. Each security team member should know in detail the security features provided by the equipment in his or her operational area.

While we have defined the responsibilities of the team as a whole, you should define the individual roles and responsibilities of the security team members in your security policy.

Prevention

Prevention can be broken into two parts: approving security changes and monitoring security of your network.

Approving Security Changes

Security changes are defined as changes to network equipment that have a possible impact on the overall security of the network. Your security policy should identify specific security configuration requirements in non-technical terms. In other words, instead of defining a requirement as "No outside sources FTP connections will be permitted through the firewall", define the requirement as "Outside connections should not be able to retrieve files from the inside network". You'll need to define a unique set of requirements for your organization.

The security team should review the list of plain language requirements to identify specific network configuration or design issues that meet the requirements. Once the team has created the required network configuration changes to implement the security policy, you can apply these to any future configuration changes. While it's possible for the security team to review all changes, this process allows them to only review changes that pose enough risk to warrant special treatment.

We recommend that the security team review the following types of changes:

- Any change to the firewall configuration.
- Any change to access control lists (ACL).
- Any change to Simple Network Management Protocol (SNMP) configuration.
- Any change or update in software that differs from the approved software revision level list.

We also recommend adhering to the following guidelines:

- Change passwords to network devices on a routine basis.
- Restrict access to network devices to an approved list of personnel.
- Ensure that the current software revision levels of network equipment and server environments are in compliance with the security configuration requirements.

In addition to these approval guidelines, have a representative from the security team sit on the change management approval board, in order to monitor all changes that the board

reviews. The security team representative can deny any change that is considered a security change until it has been approved by the security team.

Monitoring Security of Your Network

Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation. The starting point for security monitoring is determining what a violation is. In *Conduct a Risk Analysis*, we identified the level of monitoring required based on the threat to the system. In *Approving Security Changes*, we identified specific threats to the network. By looking at both these parameters, we'll develop a clear picture of what you need to monitor and how often.

In the Risk Analysis matrix, the firewall is considered a high-risk network device, which indicates that you should monitor it in real time. From the *Approving Security Changes* section, you see that you should monitor for any changes to the firewall. This means that the SNMP polling agent should monitor such things as failed login attempts, unusual traffic, changes to the firewall, access granted to the firewall, and connections setup through the firewall.

Following this example, create a monitoring policy for each area identified in your risk analysis. We recommend monitoring low-risk equipment weekly, medium-risk equipment daily and high-risk equipment hourly. If you require more rapid detection, monitor on a shorter time frame.

Lastly, your security policy should address how to notify the security team of security violations. Often, your network monitoring software will be the first to detect the violation. It should trigger a notification to the operations center, which in turn should notify the security team, using a pager if necessary.

Response

Response can be broken into three parts: security violations, restoration, and review.
Security Violations

When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable.

The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to apply the correct response. Define a procedure in your security policy that is available 24 hours a day, 7 days a week.

Next you should define the level of authority given to the security team to make changes, and in what order the changes should be made. Possible corrective actions are:

- Implementing changes to prevent further access to the violation.
- Isolating the violated systems.

- Contacting the carrier or ISP in an attempt to trace the attack.
- Using recording devices to gather evidence.
- Disconnecting violated systems or the source of the violation.
- Contacting the police, or other government agencies.
- Shutting down violated systems.
- Restoring systems according to a prioritized list.
- Notifying internal managerial and legal personnel.

Be sure to detail any changes that can be conducted without management approval in the security policy.

Lastly, there are two reasons for collecting and maintaining information during a security attack: to determine the extent to which systems have been compromised by a security attack, and to prosecute external violations. The type of information and the manner in which you collect it differs according to your goal.

To determine the extent of the violation, do the following:

- Record the event by obtaining sniffer traces of the network, copies of log files, active user accounts, and network connections.
- Limit further compromise by disabling accounts, disconnecting network equipment from the network, and disconnecting from the Internet.
- Backup the compromised system to aid in a detailed analysis of the damage and method of attack.
- Look for other signs of compromise. Often when a system is compromised, there are other systems or accounts involved.
- Maintain and review security device log files and network monitoring log files, as they often provide clues to the method of attack.

If you're interested in taking legal action, have your legal department review the procedures for gathering evidence and involvement of the authorities. Such a review increases the effectiveness of the evidence in legal proceedings. If the violation was internal in nature, contact your Human Resources department.

Restoration

Restoration of normal network operations is the final goal of any security violation response. Define in the security policy how you conduct, secure, and make available normal backups. As each system has its own means and procedures for backing up, the security policy should act as a meta-policy, detailing for each system the security conditions that require restoration from backup. If approval is required before restoration can be done, include the process for obtaining approval as well.

Review

The review process is the final effort in creating and maintaining a security policy. There are three things you'll need to review: policy, posture, and practice.

The security policy should be a living document that adapts to an ever-changing environment. Reviewing the existing policy against known Best Practices keeps the network up to date. Also, check the CERT web site leavingcisco.com CERT web site for useful tips, practices, security improvements, and alerts that can be incorporated into your security policy.

You should also review the network's posture in comparison with the desired security posture. An outside firm that specializes in security can attempt to penetrate the network and test not only the posture of the network, but the security response of your organization as well. For high-availability networks, we recommend conducting such a test annually.

Finally, practice is defined as a drill or test of the support staff to insure that they have a clear understanding of what to do during a security violation. Often, this drill is unannounced by management and done in conjunction with the network posture test. This review identifies gaps in procedures and training of personnel so that corrective action can be taken.

3.0 SITE OPERATIONS OVERVIEW

3.1 Document Maintenance Best Practices

SPIRIT WIC software is best viewed by client PC utilizing Internet Explorer 5.5 or greater on Windows XP.

To maintain optimal performance of Windows XP, the following steps should be taken.

- 1) Set Windows Update to Automatically download and install patches every night
- 2) Defrag your hard disk every week by selecting Start -> Programs -> Accessories -> System Tools -> Disk Defragmenter. Highlight your Hard Drive (usually c) and click the 'Defragment Button' at the bottom left of the window.
- 3) Schedule your Anti-Virus program to run a full scan nightly.
- 4) Install Anti-Spyware program if not included with your Antivirus – schedule to run a full scan nightly.

3.2 Document Communication Requirements

We recommend finding a local ISP provider to determine types of Internet connection speeds that are available at each site. Below is a list of recommended connections based on the number of simultaneous users, but not availability of service by ISP.

User Qty	ISP Service	Device
1-2	POTS / Dial Up	3COM LAN Modem
3-7	DSL / Cable	Cable/DSL Modem, Router/Switch with DHCP and Firewall
7 or more	Fractional T1 / T1	Router / Switch with DHCP and Firewall (possibly sourced from T1 Service Provider)

3.3 Document Troubleshooting FAQ

Q. I am unable to get to the Arkansas SPIRIT software website; I connected fine yesterday, what happened?

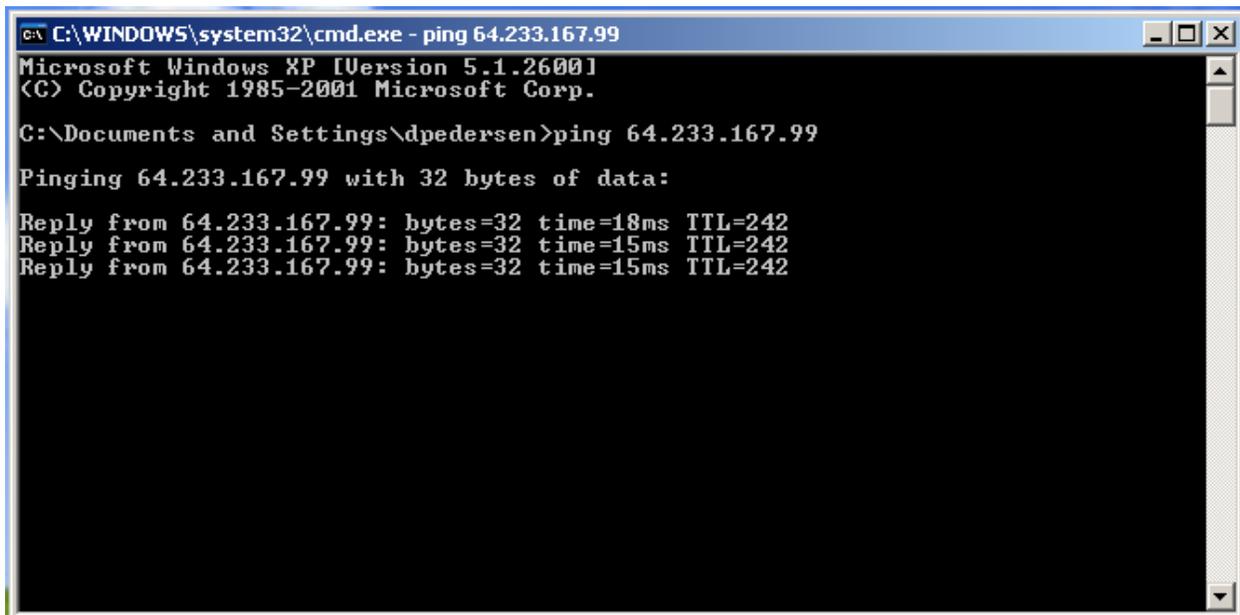
A. The first step is to see if you can connect to any other web sites with your web site browser, try going to www.google.com or www.yahoo.com.

If you can connect to those web sites, see if another computer in your office has trouble connecting to the application. If they are unable to connect, call the ADH Help Desk.

Ping Test

If you are unable to connect to other web sites, we will need to first do a ping test to check connectivity.

- Click 'Start' select 'Run' type 'CMD' and press the enter key.
- When you see the dos command prompt, type **ping 64.233.167.99** and hit enter
- If the response reads something like 'Reply from 64.233.167.99: bytes = 32 time=15ms TTL=242' you know you have a good network connection.
- Next try typing '**ping google.com**'. If the response reads something like 'Reply from 64.233.167.99: bytes = 32 time=15ms TTL=242' you know DNS is working. Try going to the SPIRIT web site again. If you are unsuccessful you should call the help desk.



```
C:\WINDOWS\system32\cmd.exe - ping 64.233.167.99
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dpedersen>ping 64.233.167.99

Pinging 64.233.167.99 with 32 bytes of data:

Reply from 64.233.167.99: bytes=32 time=18ms TTL=242
Reply from 64.233.167.99: bytes=32 time=15ms TTL=242
Reply from 64.233.167.99: bytes=32 time=15ms TTL=242
```

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dpedersen>ping google.com

Pinging google.com [64.233.167.99] with 32 bytes of data:

Reply from 64.233.167.99: bytes=32 time=42ms TTL=242
Reply from 64.233.167.99: bytes=32 time=50ms TTL=242
Reply from 64.233.167.99: bytes=32 time=15ms TTL=242
Reply from 64.233.167.99: bytes=32 time=16ms TTL=242

Ping statistics for 64.233.167.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 50ms, Average = 30ms

C:\Documents and Settings\dpedersen>
```

- When attempting to ping by IP address 24.233.167.99 or google.com you receive an error message that says 'Destination host unreachable', you are probably not connected to the internet.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dpedersen>ping 24.233.167.99

Pinging 24.233.167.99 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 24.233.167.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\dpedersen>_
```

Check the network cable in the back of your computer to ensure it's still plugged in. The network cable looks similar to a phone cable with a larger end. Please make sure this is pushed all the way in to the network card.



After plugging it in, you may see lights blinking in the back of your network card. If so, try the ping test again as described above.

If the ping test doesn't work, you may need to reset your Cable/DSL modem and router. Your office connects to the internet either by Telephone Modem, Cable or DSL Modem, or a special T-1 connection.

Telephone Modem

If you are connected by Telephone Modem, confirm that the AC adapter, phone cords, and network cables are all plugged in securely and into their assigned ports. Power cycle the modem by turning it off, or unplugging it. Wait 20 seconds then turn it back on. Click 'Start' select 'Run' type 'cmd' and hit the Enter key. Type `ipconfig/release` wait for a response, then click `ipconfig/renew`. Try again to connect to the SPIRIT software. If you are unable to connect to the SPIRIT software, and the ping test doesn't work, you will need to contact your help desk.

Cable or DSL Modem

If you are connected by Cable or DSL Modem, confirm that the AC adapter, phone cords, and network cables are all plugged in securely and into their assigned ports. Power cycle the cable/DSL modem by unplugging it. Next, turn off the accompanying router by unplugging it. Wait 20 seconds and plug in the cable/DSL modem, then plug in the router. After starting both back up, wait 20 seconds. Click 'Start' select 'Run' type 'cmd' and hit the Enter key. Type `ipconfig/release` wait for a response, then click `ipconfig/renew`. Try again to connect to the SPIRIT software. If you are unable to connect to the SPIRIT software, and the ping test doesn't work, you will need to contact your help desk.

T1 or Fractional T1

If you are connected through a T-1 or Fractional T-1 service, confirm that the AC adapter and network cables are all plugged in securely and into their assigned ports on the router. Power cycle the router by unplugging it. Wait 20 seconds and plug the router back in. Click 'Start' select 'Run' type 'cmd' and hit the Enter key. Type `ipconfig/release` and wait for a response, then click `ipconfig/renew`. Try again to connect to the SPIRIT software. If you are unable to connect to the SPIRIT software, and the ping test doesn't work, you will need to contact your help desk.

4.0 APPENDICIES

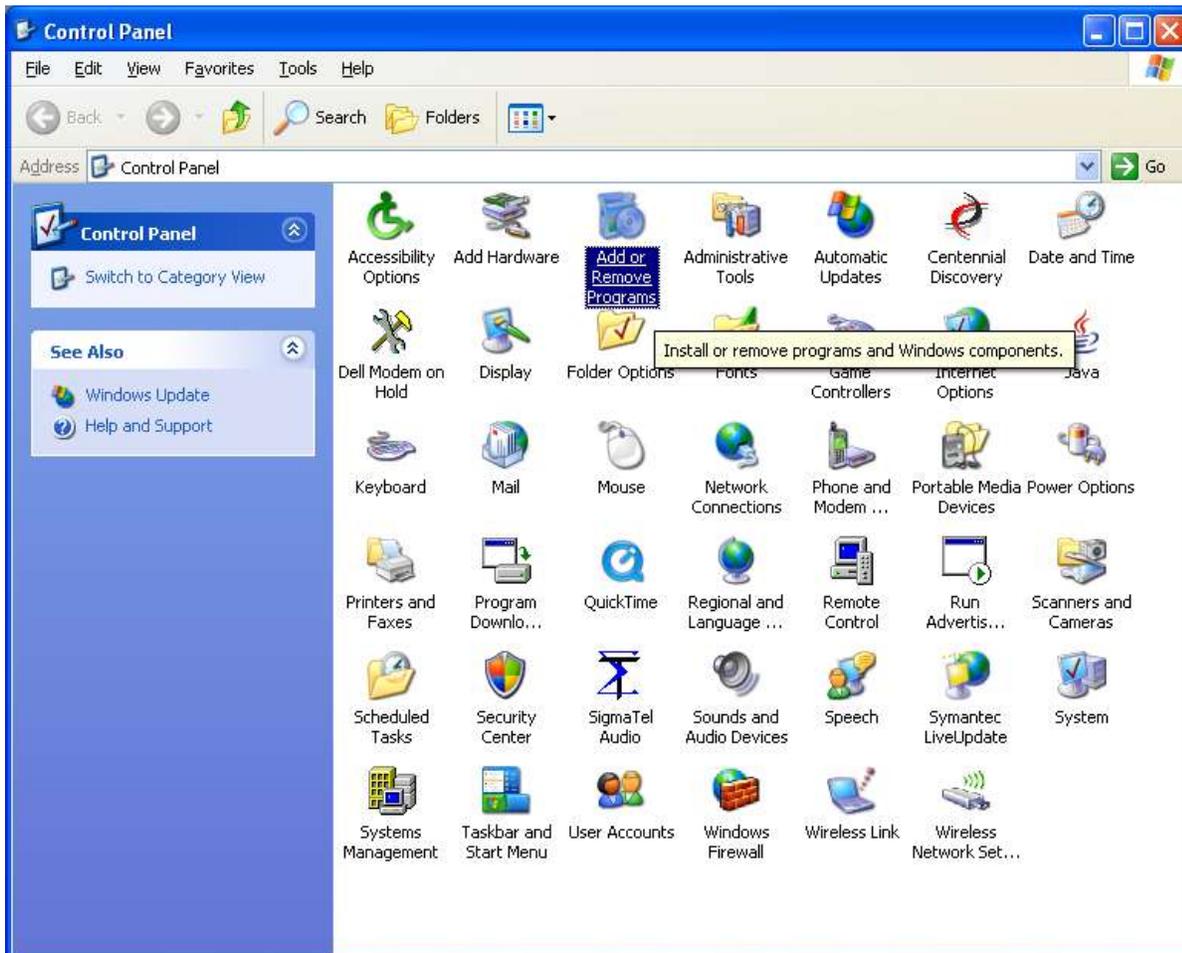
APPENDIX A – INSTALLATION INSTRUCTIONS

Installation Instructions

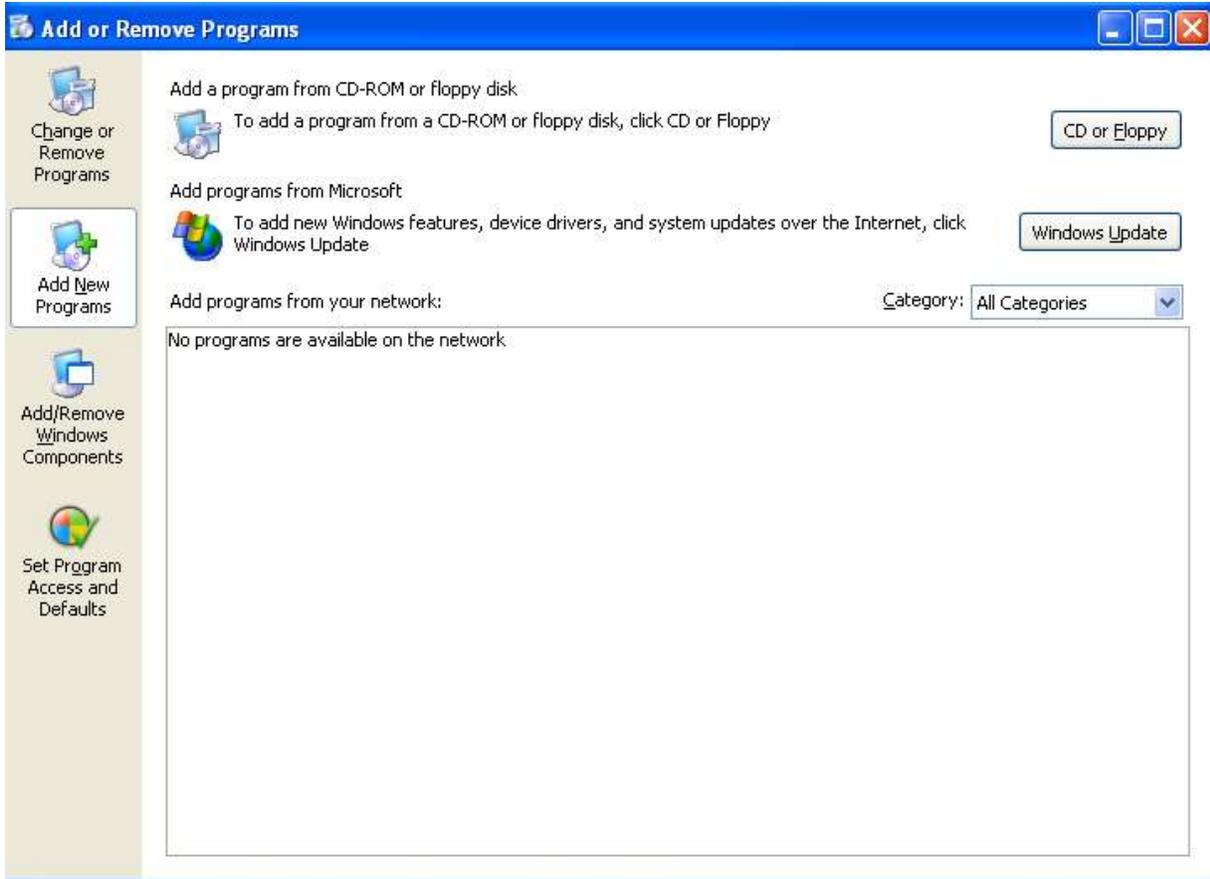
The following is a detailed description of the procedures that must be followed to complete the Spirit Installation process.

Web Server Install

Open Add or Remove Programs from the control Panel



Click the Add New Programs button on the left then select the CD or Floppy button in the top right corner



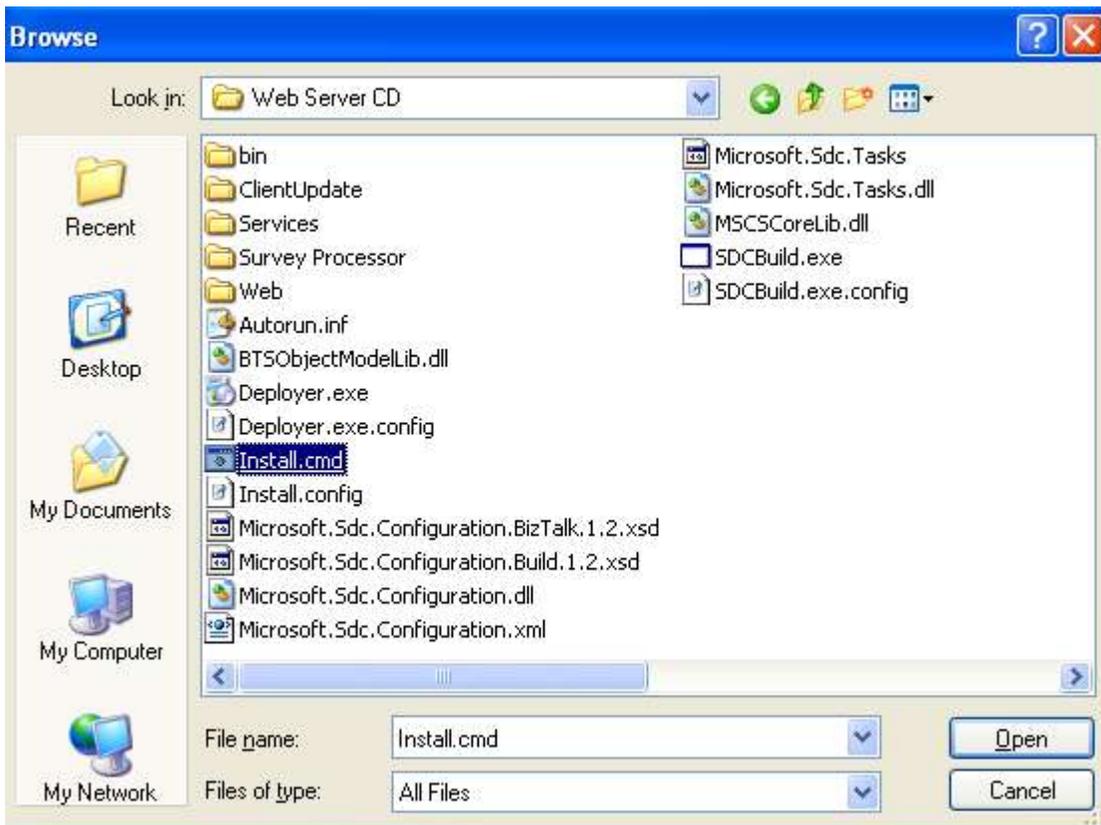
Click the Next button



Now click the Browse button



Now find the Web Server folder on the CD and select the Install.cmd file and Click Open.
Note: the “Files of type” must be set to “All Files”



Now click Finish. This will start the install.



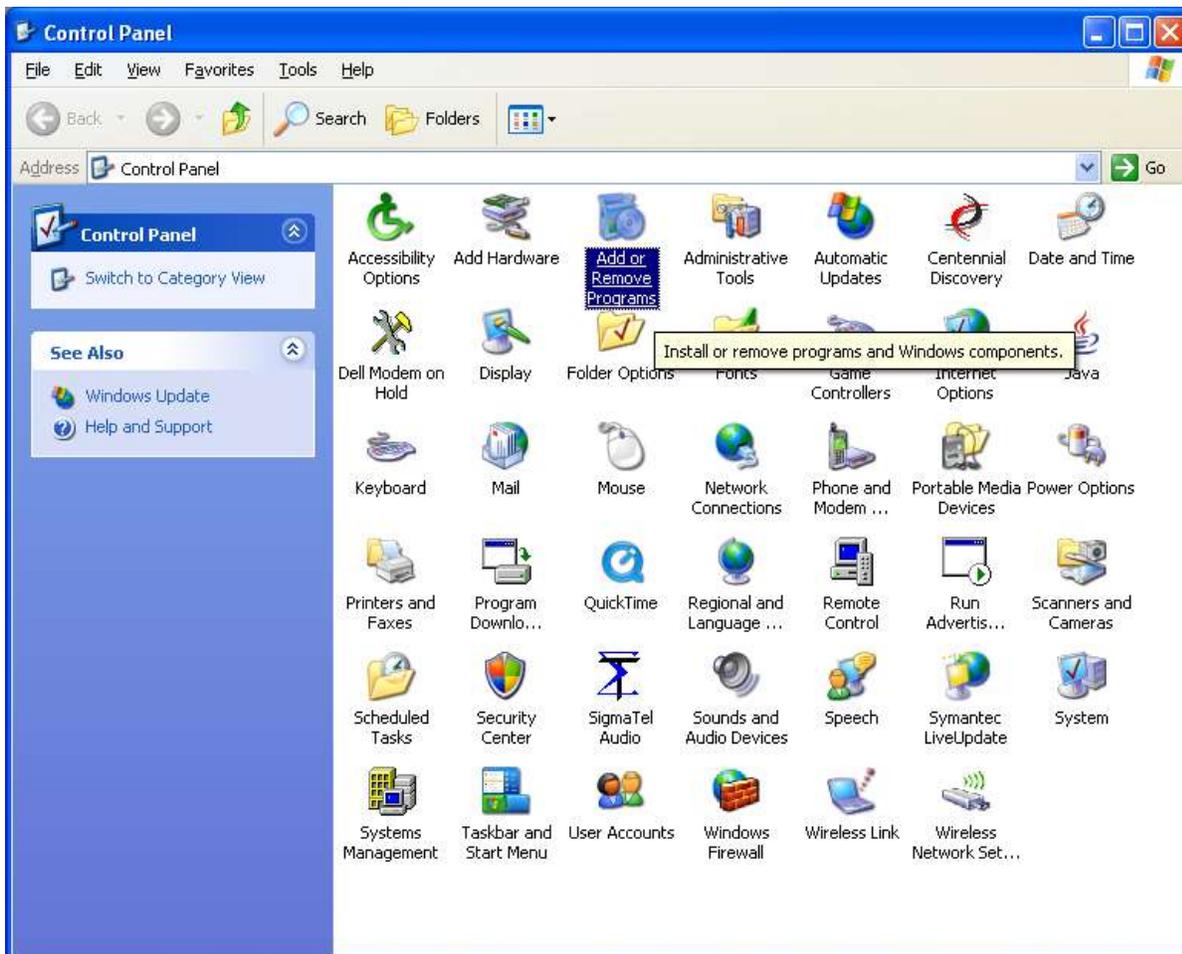
When the install is finished click "OK"



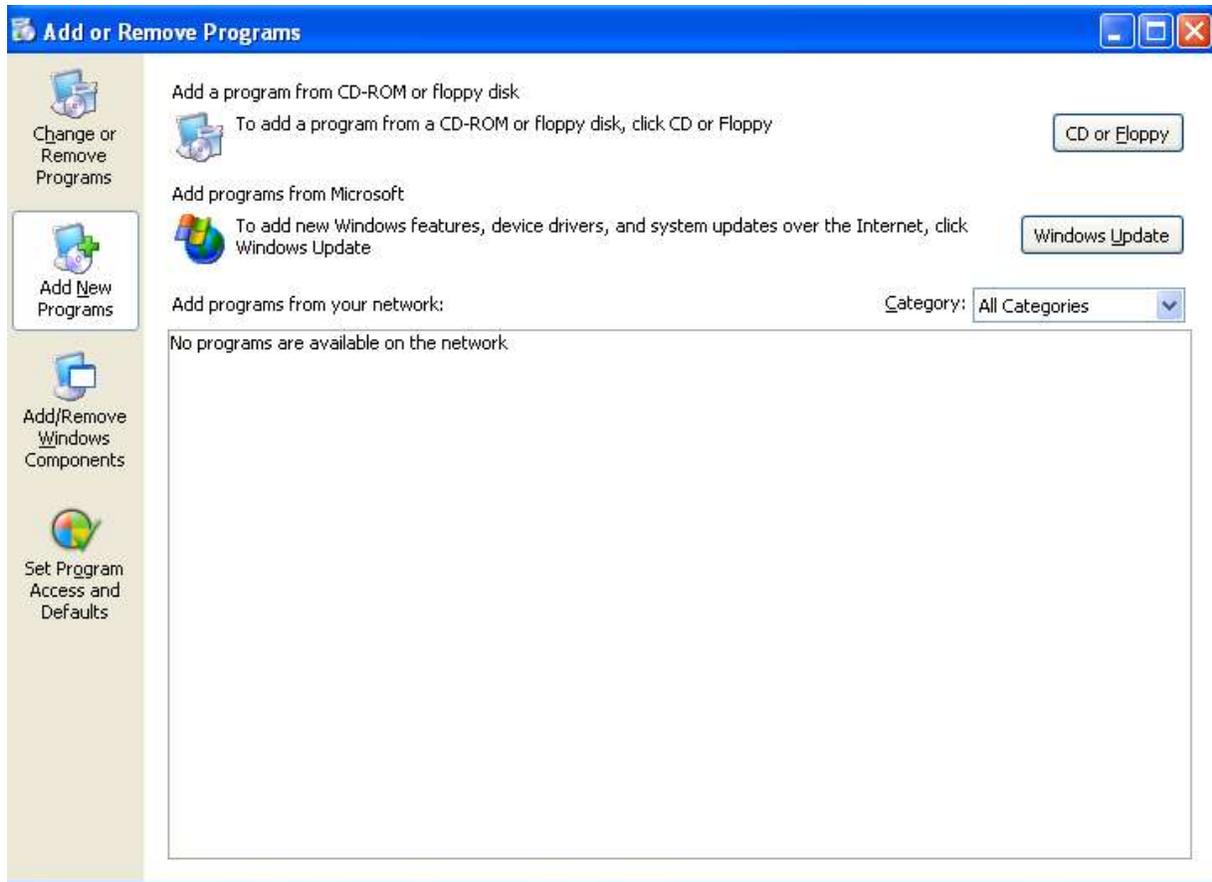
Client Install

This is for the initial install. After this install the client application will automatically check for updates on the web server.

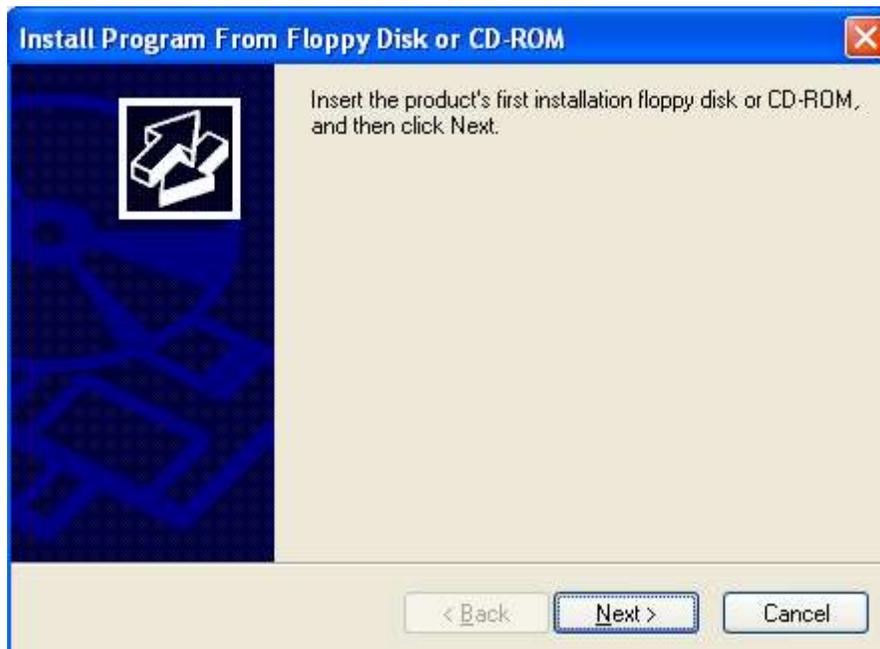
Open Add or Remove Programs from the control Panel



Click the Add New Programs button on the left then select the CD or Floppy button in the top right corner



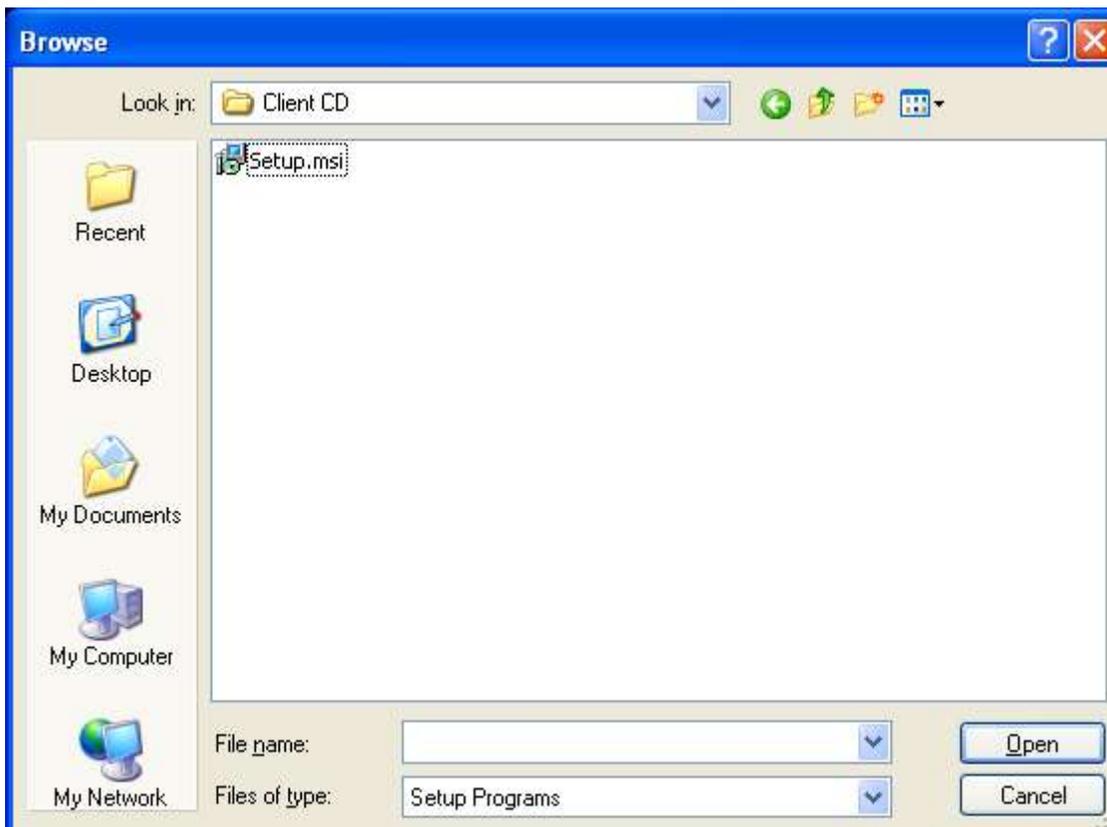
Click the Next button



Now click the Browse button



Now find the Client folder on the CD and select the Setup.msi file and Click Open.



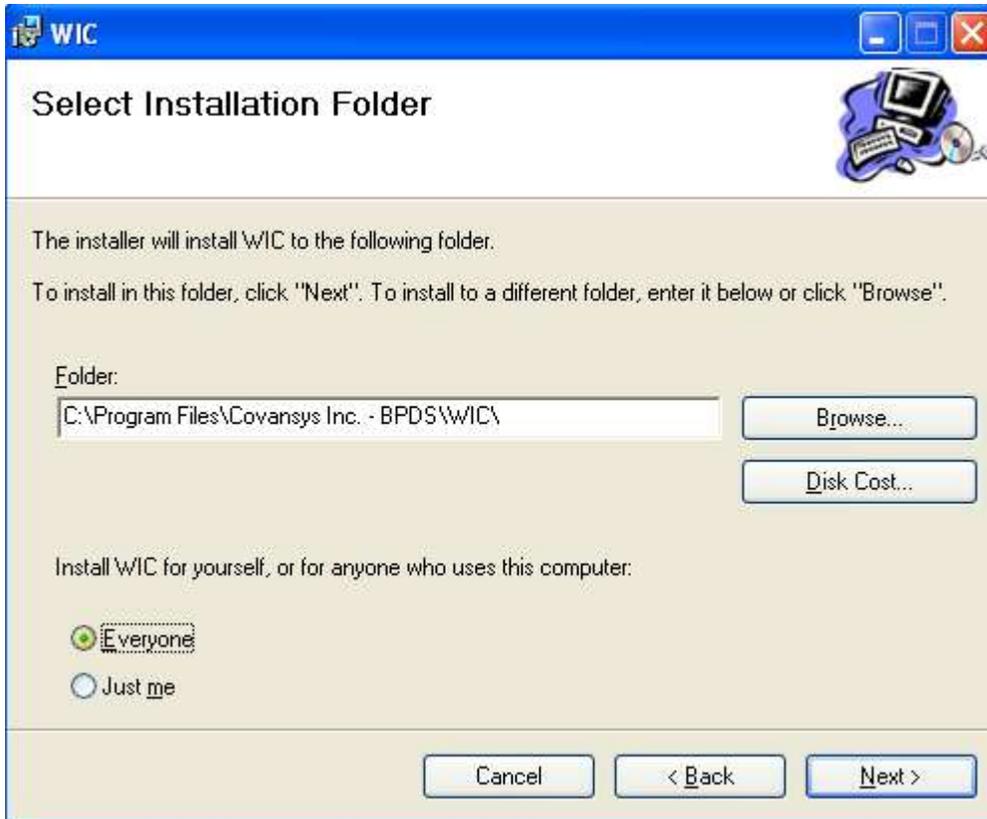
Now click Finish. This will start the install.



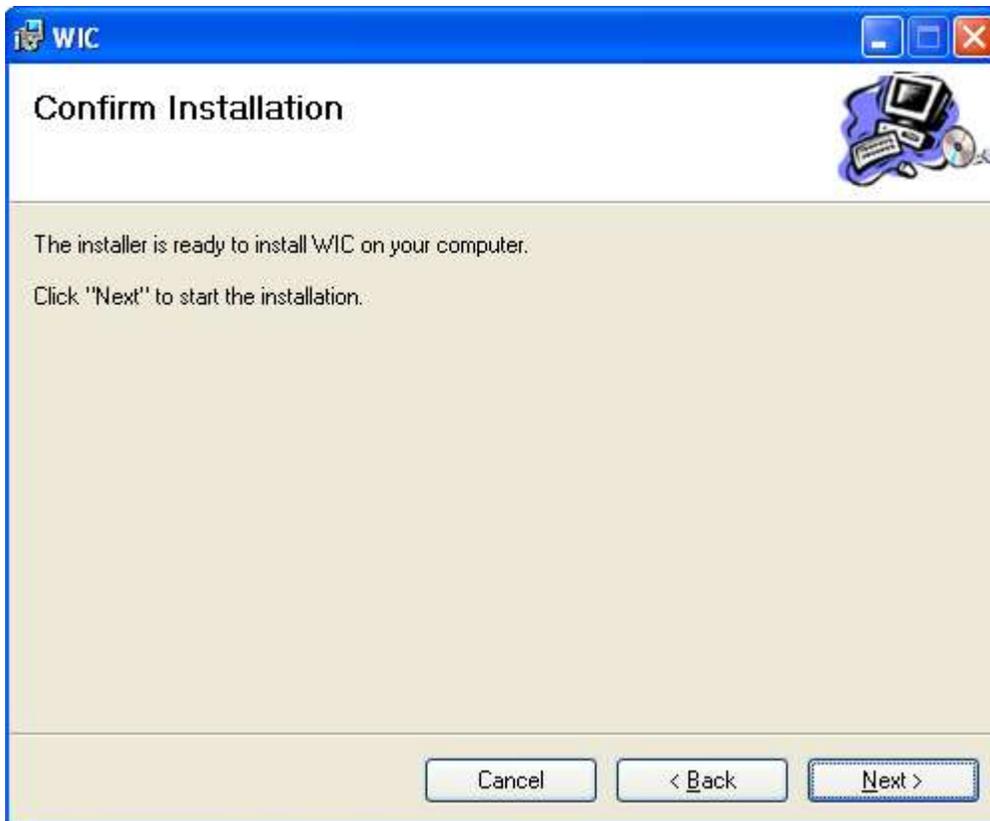
Click Next



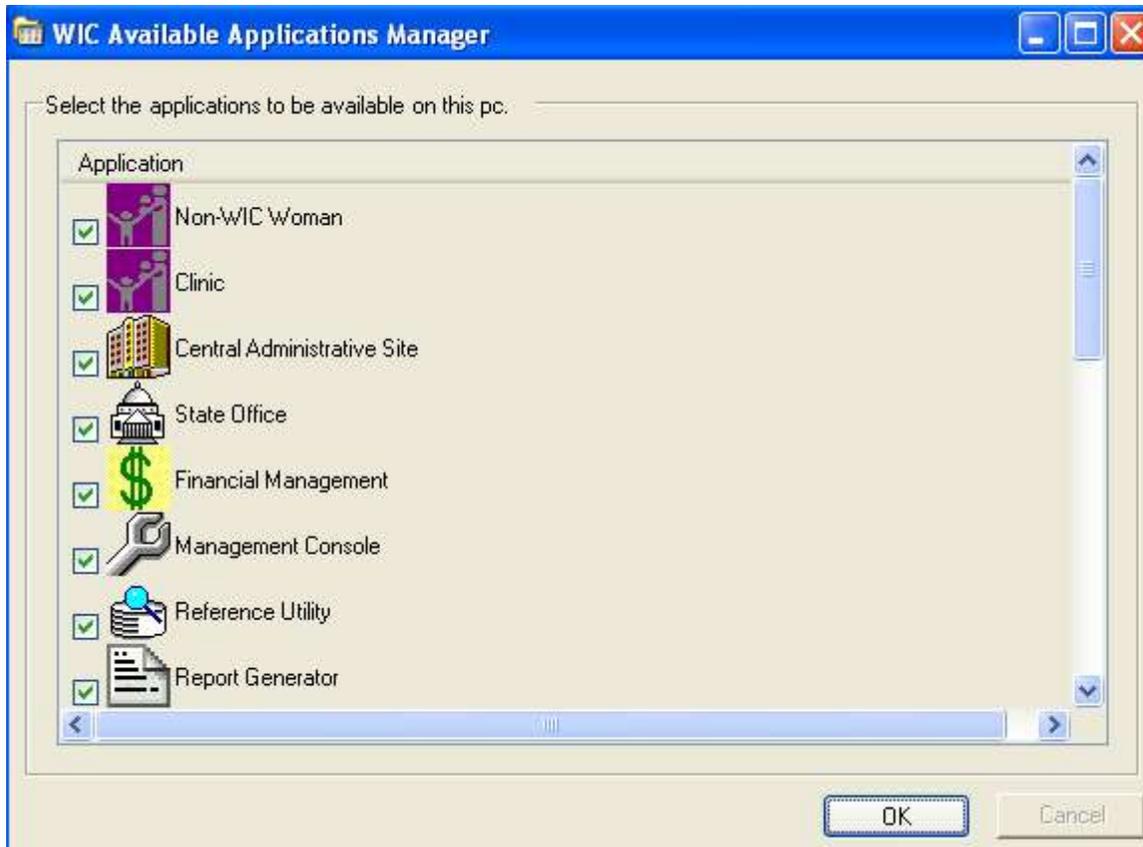
Click the “Everyone” and then click “Next”



Click Next button. This will start the install.



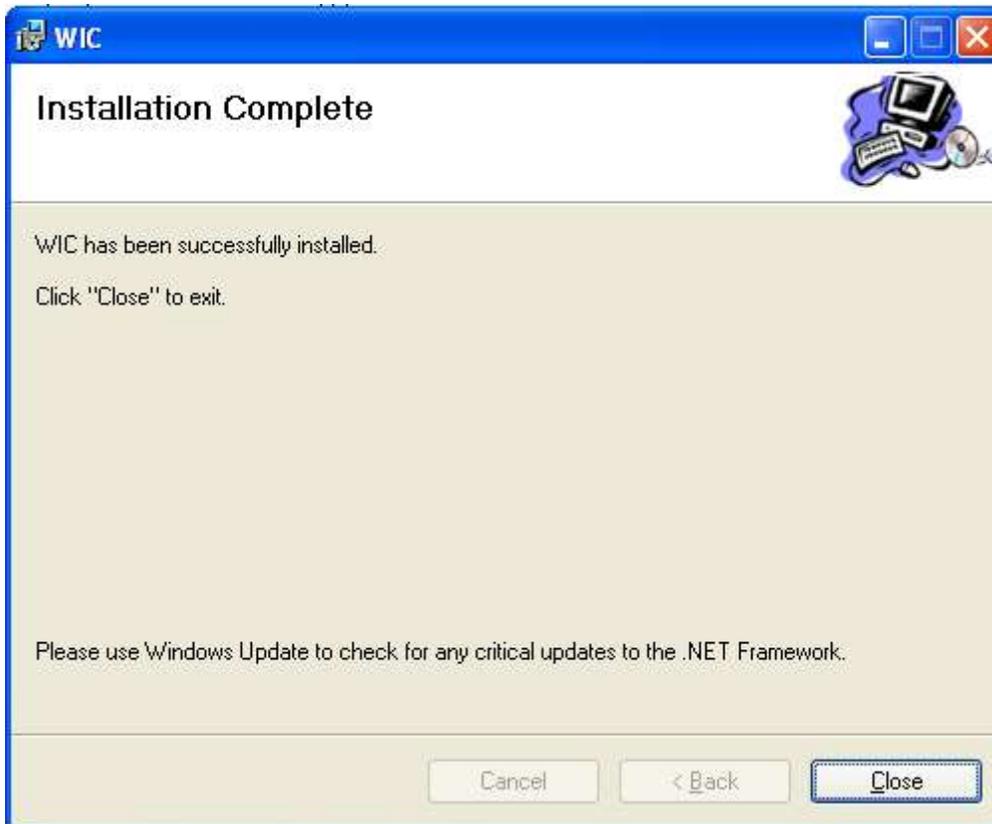
Select the applications to be available on the pc and then click OK



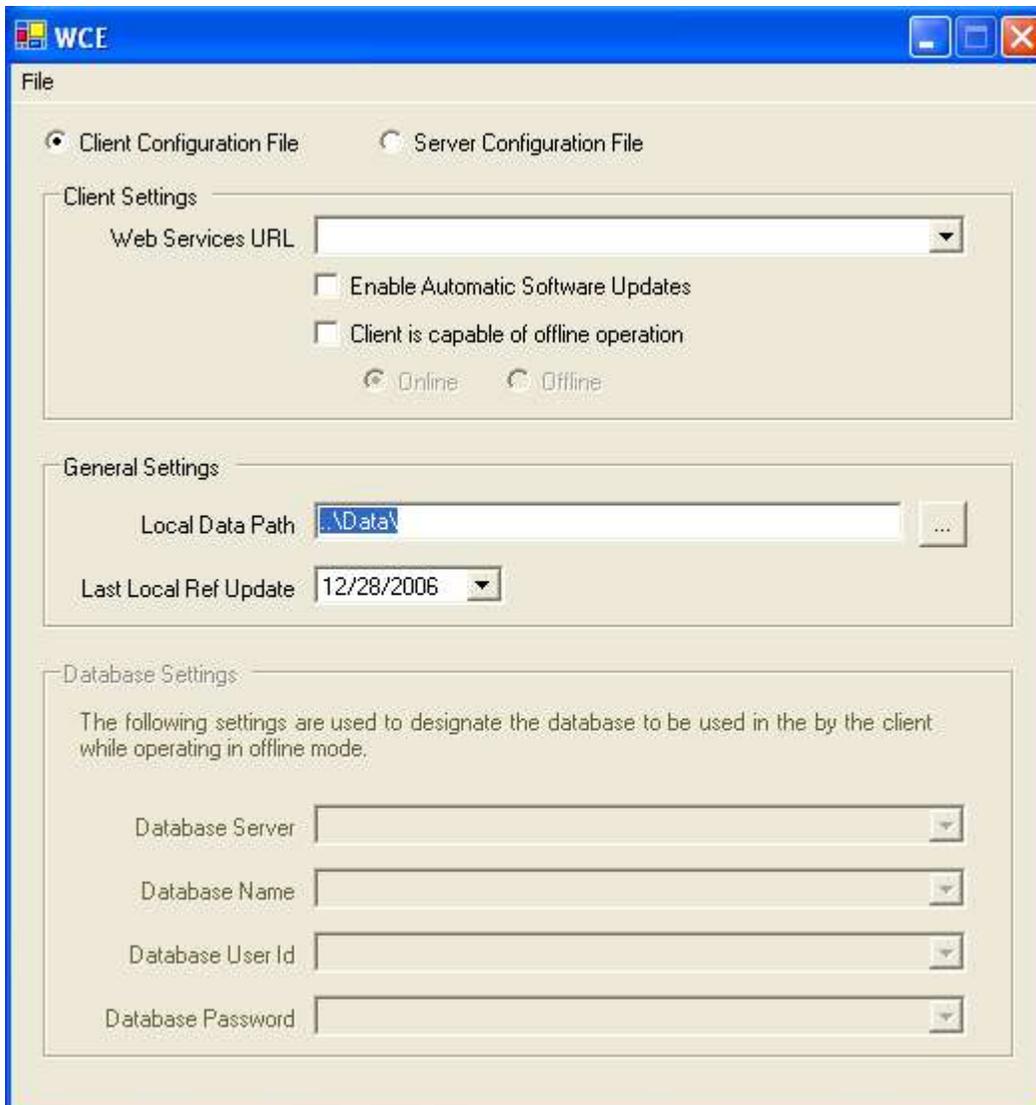
Click OK



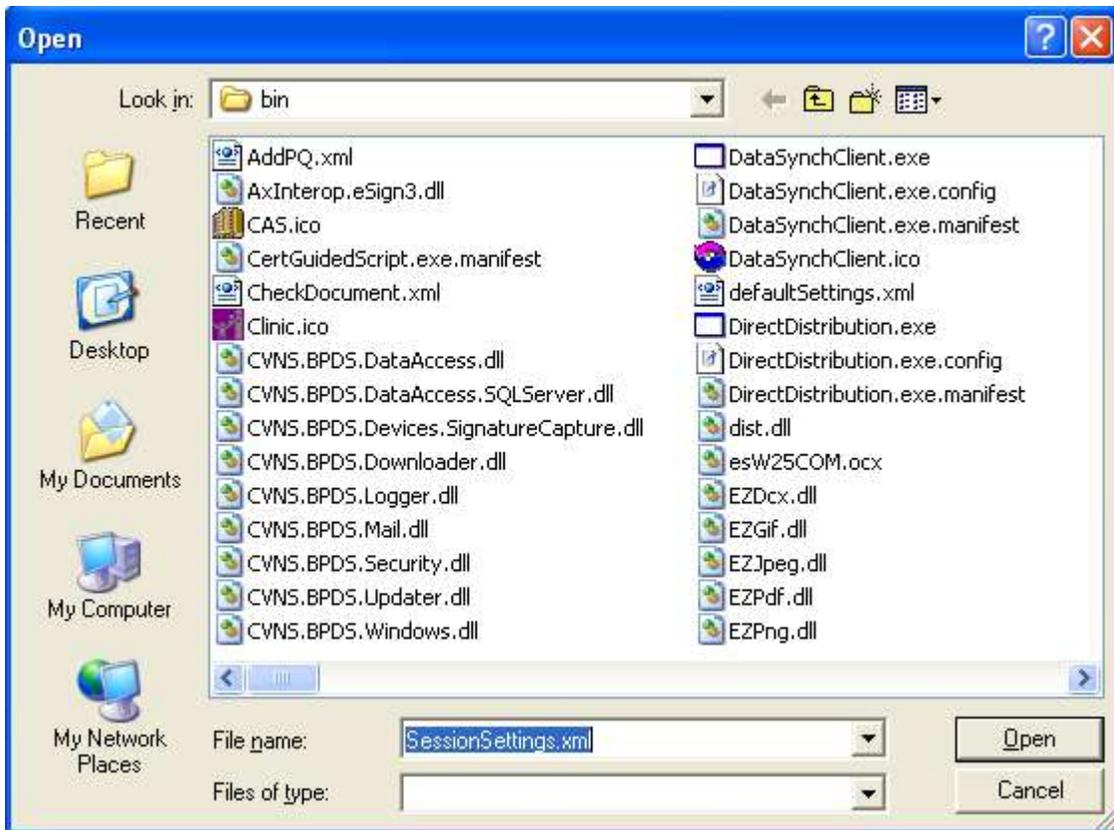
Click Close



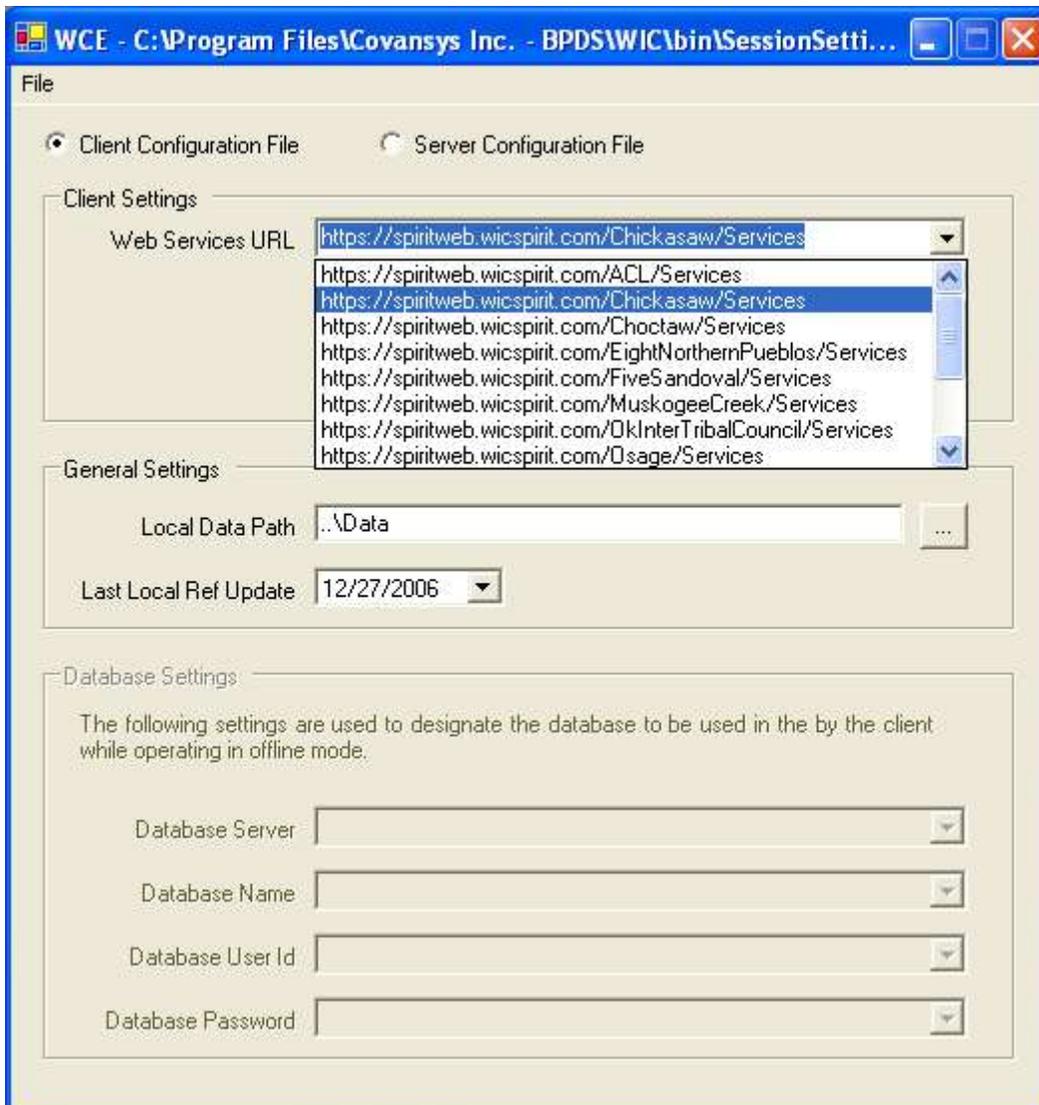
Once the install is complete open the WIC Config Editor. This is located in "Start -> All Programs -> WIC Applications -> WIC Config Editor" Select File -> Open from this screen.



Next click Open



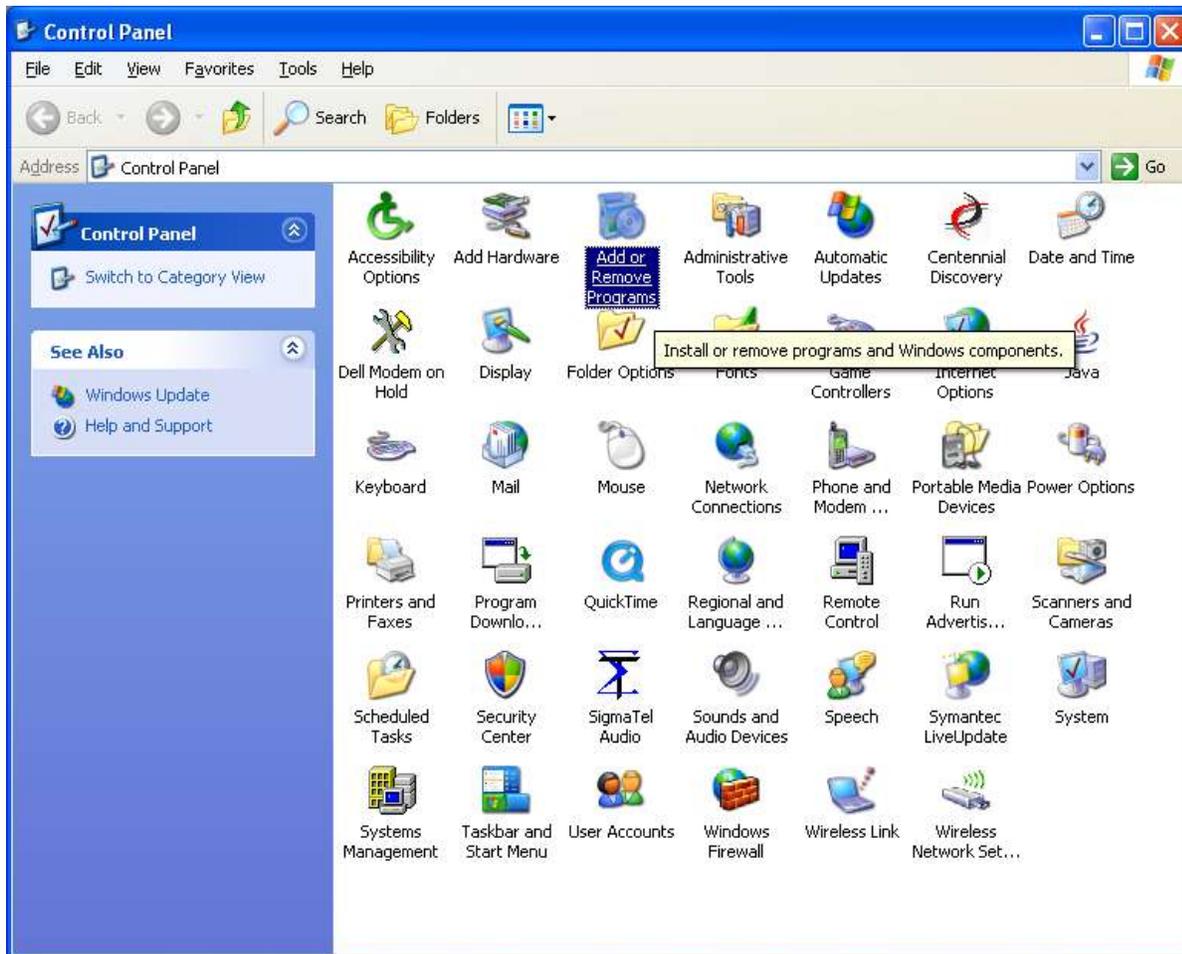
Next select the correct URL based on the State you wish to connect too. Once that is done click “File -> Save” and then exit.



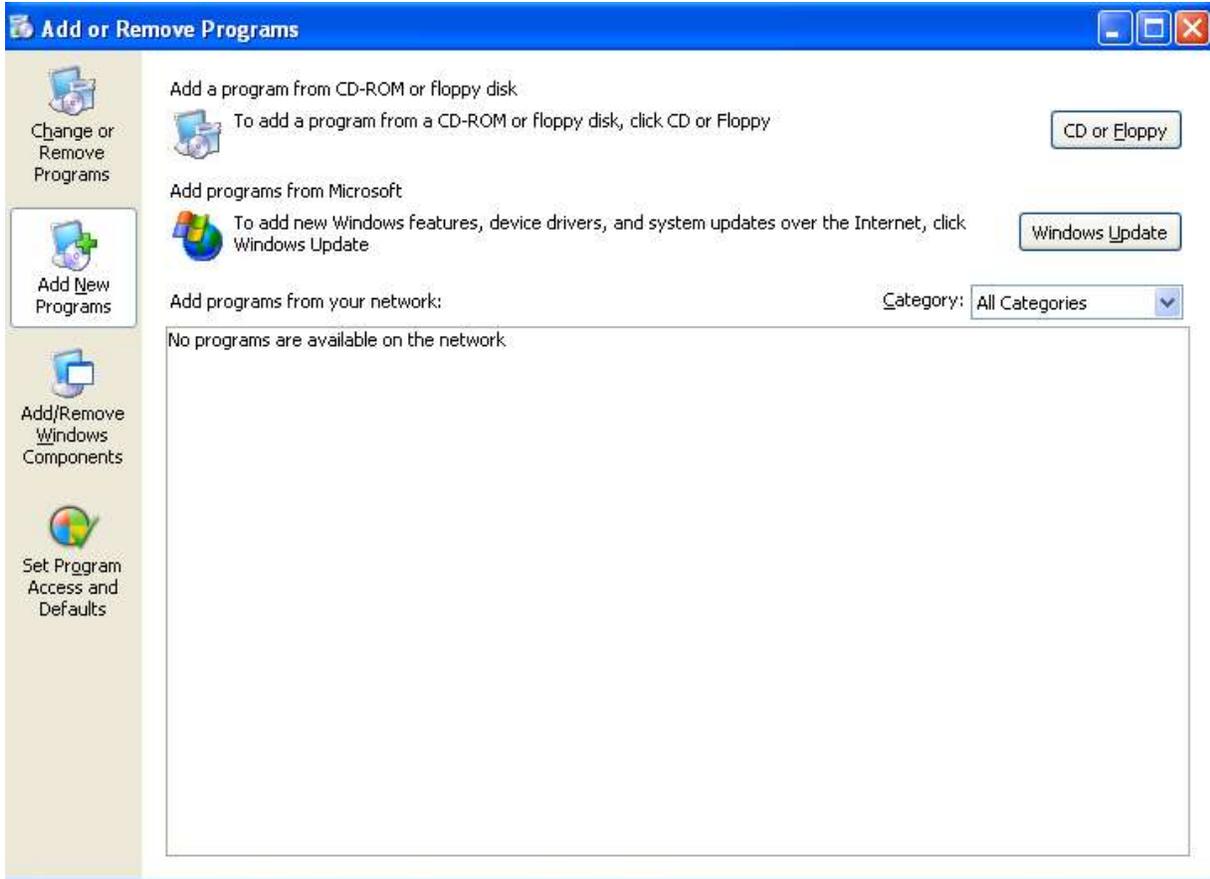
Application Server Install

For the first time setup the following bat file needs to be run: setup_dirs_app_server.bat

Open Add or Remove Programs from the control Panel



Click the Add New Programs button on the left then select the CD or Floppy button in the top right corner



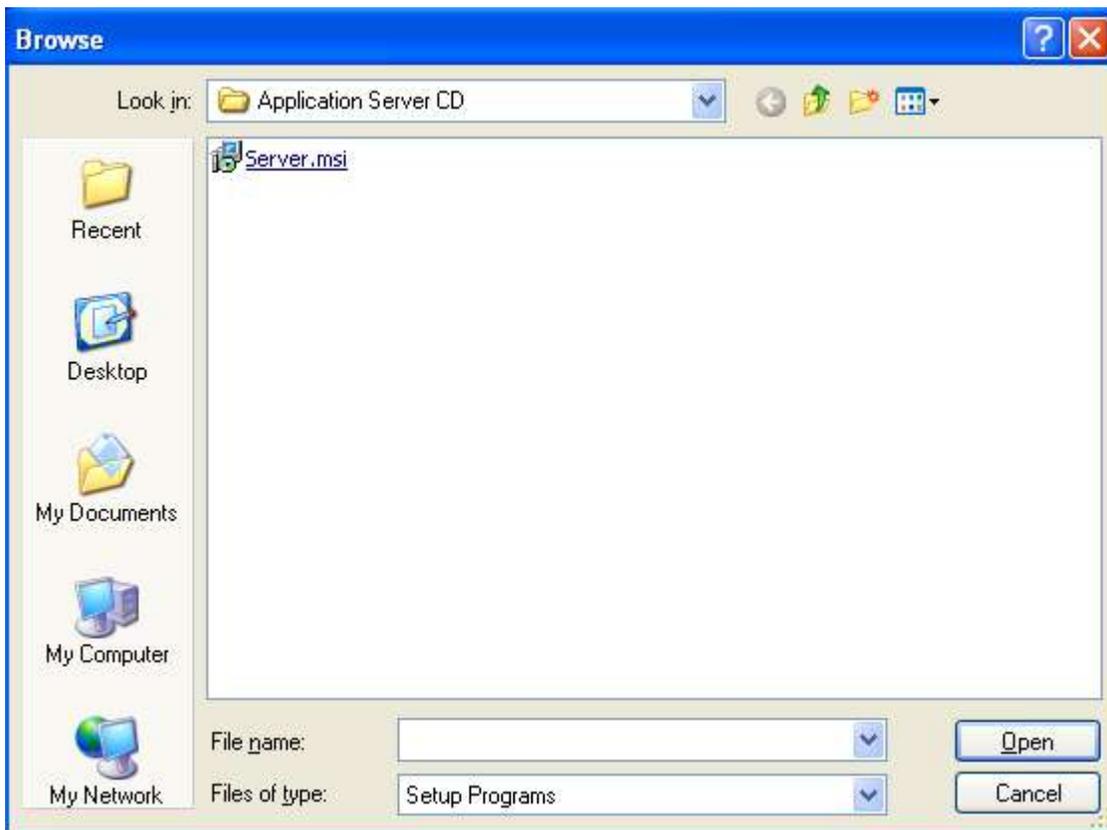
Click the Next button



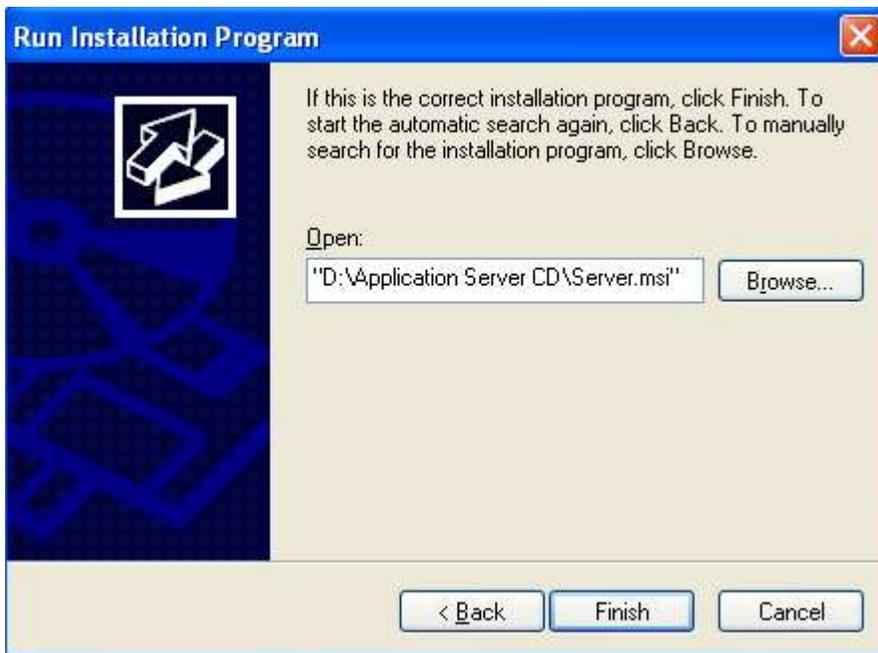
Now click the Browse button



Now find the Application Server folder on the CD and select the Server.msi file and Click Open.



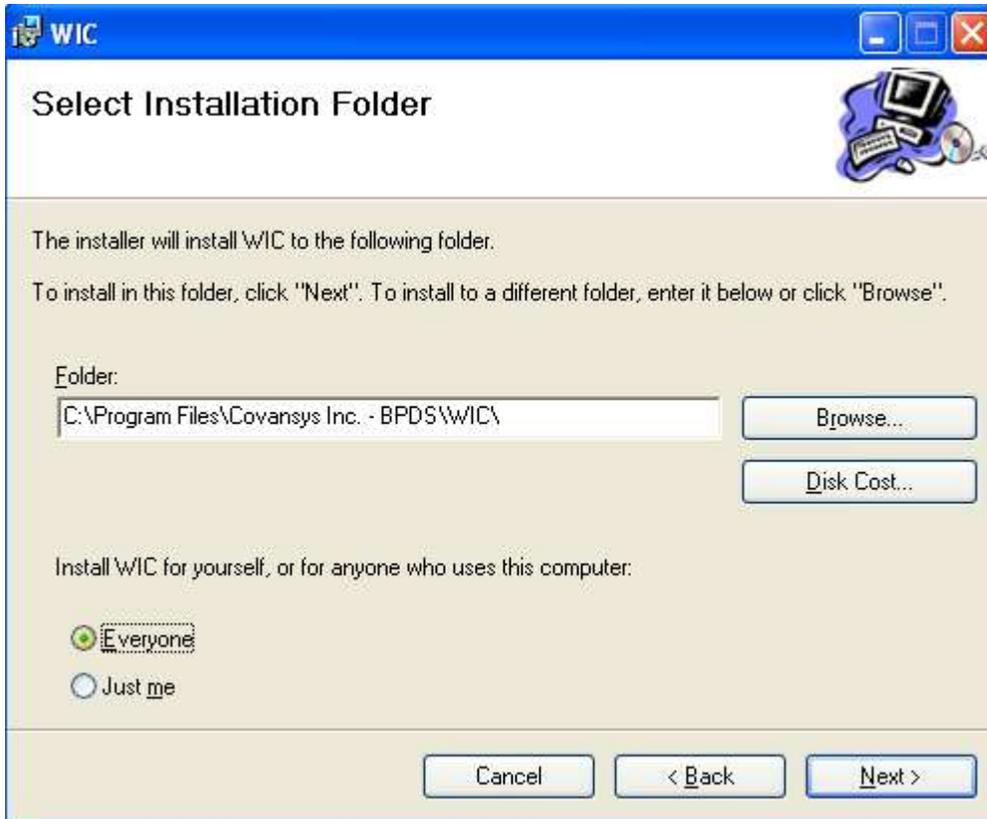
Click Finish



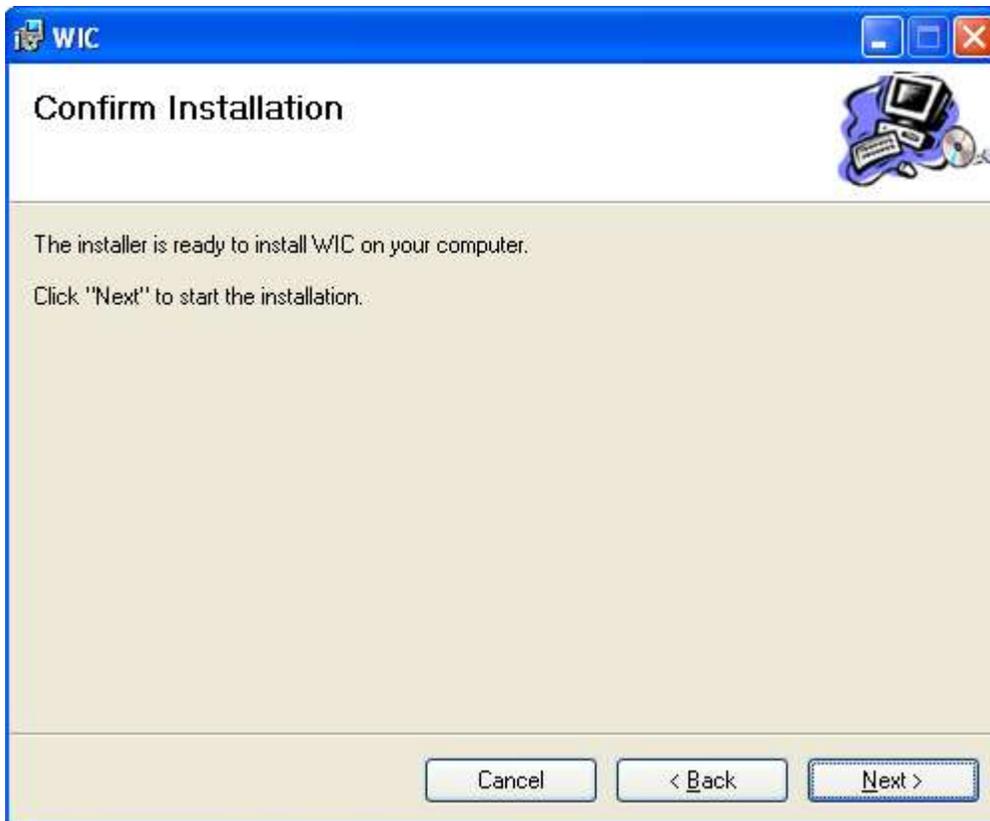
Click Next



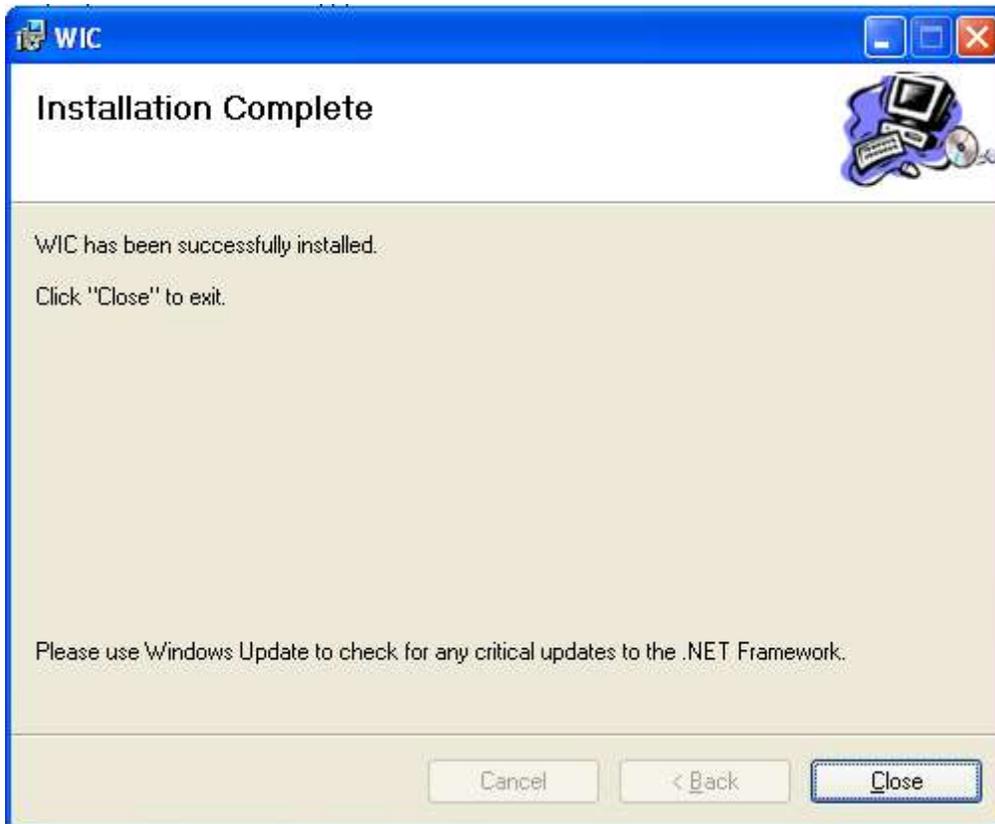
Click the “Everyone” and then click “Next”



Click Next button. This will start the install.



Click Close



Database Updates

After each refreshing the follow SQL needs to be run against the refreshed schema:

```
sp_change_users_login 'update_one', 'spirit', 'spirit'  
go
```

APPENDIX B – DISASTER RECOVERY PLAN

Note: See Arkansas WIC Project, Disaster Recovery Plan, June 9, 2008.

Plan Overview

This is the recommended IT Disaster Recovery and Business Continuity Plan for Arkansas WIC. It is to be used as a guide for ensuring the successful recovery of the Arkansas WIC operating environment in the event of a disaster. Back up and recovery procedures are documented here as are the testing methods that should be used to ensure successful recovery of the environment.

Definition of a Disaster

A disaster is any non-predicted event that significantly jeopardizes the ability of any Arkansas WIC functional site to deliver its assigned services. The following examples of major disasters are categorized as:

- Natural
 - Earthquake
 - Tornado
 - Hurricane
 - Flood
 - Lightning
 - Fire
 - Epidemic
 - Blizzard
- Labor
 - Work Slowdown
- System Issues
 - Hardware/Software Failure
 - Data Communications Outage
- Subversive Acts
 - Sabotage
 - Terrorism
- Demonstrations
 - Labor
 - Political

A disaster will be declared if the primary site is non-operational or projected to be non-operational for twenty four (24) business hours (or 24 concurrent hours for systems). The extended period allows repair time for minor 'disasters'. Examples are extended power outages within UPS and generator capacities, repairable system failures, temporary communication outages, or other 'repairable' issues. However, a disaster may be declared sooner if it is highly likely the systems or facility will not be operational within the next business day (i.e. – catastrophic loss such as fire, tornado, or earthquake).

A disaster can only be declared by the Executive Recovery Coordinator (ERC) or the Systems Recovery Coordinator (SRC). Other members of CSC Covansys management may

declare a disaster in the event that neither the ERC nor SRC is accessible for an extended period of time and a catastrophic loss has clearly occurred.

Once a disaster is declared, the designated alternate site will be prepared, the proper site coordinator will be contacted, and all appropriate disaster coordinators will be notified. The plan will begin execution as detailed for each individual location.

The system will be brought to full service as quickly as reasonably possible but is not to exceed three (3) calendar days of the original system or facility failure date and time.

Once the original location is restored to usable condition, a plan will be published scheduling the time of relocation. Such relocation will be coordinated not to impact normal business hours. Downtime to relocate systems back to permanent facilities is not to exceed 6 non-production hours and only during non-catastrophe operations.

Arkansas WIC Functional Sites

The entire Arkansas WIC service offering is actually performed by personnel and machines in several different geographical locations as shown in the following table:

Site	IT Purpose	Address
ADH Central Office	Main Network Location	4815 West Markham

Disaster Recovery Contacts

The IT Disaster Recovery Team includes ADH IT employees, customer and vendor contacts. The Disaster Recovery Team is responsible for:

- Assessing the severity of the disaster
- Assisting in the evacuation of facility personnel
- Protecting site resources
- Contacting appropriate members of management
- Collecting information necessary to determine the nature of the disaster, the extent of damage and harm, and the estimated length of interruption to operations.
- Implementing on-site/off-site disaster recovery processes

Covansys Disaster Recovery Contacts

The ADH IT Disaster Recovery team has primary responsibility for:

- 1) Declaring a disaster
- 2) Coordinating disaster recovery efforts
- 3) Ensuring failsafe operations are followed
- 4) Testing failsafe and recovery operations and reporting on test results
- 5) Keeping this plan up to date.

The following individuals make up the ADH IT Disaster Recovery team.

Jerry Pack	CIO	501-661-2180 501650-0667	Central Office, ITS
Keith Burns	Information Systems Manager	501-661-2013 501-551-9426	Central Office, ITS
Warren Bankson	Sr. Project Leader/Network Administrator	501-661-2989 501-944-2168	Central Office, ITS
Francis St. Germaine	Desktop Support Manager	501-280-4051 501-944-2156	Central Office, ITS

Customer Contacts

The ADH IT disaster recovery customer contacts have primary responsibility for:

- 1) Helping to determine when a disaster should be declared
- 2) Working with the ADH disaster recovery contacts to help provide communications to various affected parties
- 3) Assisting the ADH disaster recovery team in its recovery efforts where appropriate

The following are the designated customer contacts:

Name	Company	Phone Numbers
Marcell Jones	ADH, WIC	501-661-2598
Judy Powell	ADH, WIC	501-661-2263

Arkansas WIC Overview

ADH IT provides full hosting service for the Arkansas WIC program. This service is hosted in our data center in Little Rock, AR. The people employed use machinery and facilities primarily owned and operated by the State of Arkansas except where noted within this document.

The environment consists of multiple Intel-based servers, large-scale database hardware, and Internet communications. Common facilities include office space and standard office equipment required to perform the system and Helpdesk support.

SPIRIT is a USDA proprietary system written in a traditional web-based model using .NET. Delivery over the Internet is accomplished using Secure Hyper-text Protocols.

Arkansas WIC Operating Environment

Servers

The following table presents a logical list of the servers that make up the Arkansas WIC server environment along with a brief description of the purpose of the server and the operating system required.

Server	Operating System	Storage/CPU
ADH-WIC-APPL001 ADH-WIC-APPL002 ADH-WIC-APPL003 ADH-WIC-APPL004 ADH-WIC-APPL005	WIN 2003	
ADH-WIC-Data01	WIN 2003/SQL 2000	

Helpdesk Workstation

Typical Hardware Configuration:

- Workstation with 2 GHz Intel , 512 MB RAM and 80 GB Hard Disk

Required Software:

- Windows XP
- Recommended Arkansas helpdesk software
- Norton Antivirus
- Email

Standard Operating Procedures

All backup and critical tapes are stored offsite. Backup tapes are moved to offsite storage the next business day. The tape backup procedures include a daily incremental backup, weekly full backups, and monthly full system backups. Incremental tapes are kept for two weeks, weekly backups kept for 40 days, and monthly backups kept for one year. The backup routines are defined as:

Daily incremental: Monday through Friday, modified files are copied to tape.

Weekly Full backup: Saturday evening, all data, software, and source code libraries are copied to tape regardless if modified or not.

Monthly System Backups: A complete system image including OS and all related OS applications are copied to tape in addition to the standard weekly backup files.

Offsite storage is managed and provided by:

ADH stores Backup up tapes DHHS office on Spring St

Recovery Procedures

Recover Arkansas WIC Servers at DR site

All production server backup tapes will be retrieved from our offsite storage and restored to the QA server located at the Little Rock, AR Disaster Recovery site. Adjustment to server IP's will be made to reflect new environment. All system functionality will be tested and then made available to Arkansas WIC clinics and state office.

APPENDIX C – GLOSSARY OF TERMS

ADMINISTRATOR

For Windows XP Professional, a person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, and helping users with networking problems. Administrators are members of the Administrators group and have full control over the domain or computer.

For Windows XP Home Edition, a person who can make system-wide changes to the computer, install software, and who has access to all files on the computer. A person with a computer administrator account has full access to other user accounts on the computer.

ALPHANUMERIC

Alphabetic and numeric characteristics (letters and numbers).

APPLICATION

A collection of one or more interrelated data processing operations set up to run on a computer on a routine, periodic basis to satisfy a particular functional need.

APPLICATION SOFTWARE

A computer program or set of programs (system) that perform a specific task (such as word processing).

ASCII

American Standard Code for Information Interchange. Standard digital set used for representing information in microcomputers.

AUTHORIZATION

The process that determines what a user is permitted to do on a computer system or network.

BACKGROUND

The screen background image used on a graphical user interface such as Windows. Any pattern or picture that can be stored as a bitmap (.bmp) file can be set as a screen background.

BACKGROUND PROGRAM

A program that runs while the user is working on another task. The computer's microprocessor assigns fewer resources to background programs than foreground programs.

BACKUP COPY

Duplicate copy of data or information stored separately in case of loss or damage to the original.

BOOT

The process of starting or resetting a computer. When first turned on (cold boot) or reset (warm boot), the computer runs the software that loads and starts the computer's operating system, which prepares it for use.

BROWSER

Software that interprets the markup of files in HTML, formats them into Web pages, and displays them to the end user. Some browsers also permit end users to send and receive e-mail, read newsgroups, and play sound or video files embedded in Web documents.

CD

A disk drive that stores and reads data from a compact disk.

CD-R

Recordable compact disc. Data can be copied to the CD on more than one occasion; however, data cannot be erased from the CD.

CD-RW

Rewritable compact disc. Data can be copied to the CD on more than one occasion and can be erased.

CHARACTER MODE

A display mode in which the monitor can display letters, numbers, and other text characters, but no graphical images or character formatting (italics, superscript, and so on).

CLIENT

Any computer or program connecting to, or requesting the services of, another computer or program. Client can also refer to the software that enables the computer or program to establish the connection.

For a local area network (LAN) or the Internet, a computer that uses shared network resources provided by another computer (called a server).

CLIENT APPLICATION

A Windows-based application that can display and store linked or embedded objects. For distributed applications, the application that imitates a request to a server application.

COMPUTER ACCOUNT

An account that is created by a domain administrator and uniquely identifies the computer on the domain. The Windows computer account matches the name of the computer joining the domain.

COMPUTER ADMINISTRATOR

A user who manages a computer. The computer administrator makes system-wide changes to the computer, including installing programs and accessing all files on the computer, and can create, change and delete the accounts of other users.

CONNECT

To assign a drive letter, port, or computer name to a shared resource so that you can use it.

CPU

Central Processing Unit. Main unit within a computer system that contains the circuits that interpret and control the execution of instructions. Directs control of information and computing.

CRASH

Hardware or software failure that renders the computer inoperative.

DAILY BACKUP

A backup that copies all selected files that have been modified the day the daily backup is performed. The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

DATA

Information that a computer processes.

DATABASE

Compilation of data records in an organized format.

DBMS

Data Base Management System. Software that manages, manipulates, and retrieves data in a database.

DEBUGGING

Process of correcting errors in a program.

DEVICE

Any piece of equipment that can be attached to a network or computer; for example, a computer, printer, joystick, adapter, or modem card, or any other peripheral equipment. Devices normally require a device driver to function with Windows.

DISK

Circular magnetic storage device which is rotated while in use. Also called a "floppy disk, hard disk or compact disk."

DISKETTE

Alternate name for 5-1/4 disks.

DISPLAY

Output device for viewing stored information.

DOCUMENT

Any self-contained piece of work created with an application program and, if saved on disk, given a unique file name by which it can be retrieved.

DOMAIN

A group of computers that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a unique name.

An Active Directory domain is a collection of computers defined by the administrator of a Windows network. These computers share a common directory database, security policies, and security relationships with other domains. An Active Directory domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. An Active Directory forest is made up of one or more domains, each of which can span more than one physical location.

A DNS domain is any tree or sub-tree within the DNS namespace. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Active Directory domains.

DOMAIN NAME

The name given by an administrator to a collection of networked computers that share a common directory. Part of the Domain Name System (DNS) naming structure, domain names consist of a sequence of name labels separated by periods.

DRIVE

An area of storage that is formatted with a file system and has a drive letter. The storage can be a floppy disk, a CD, a hard disk, or another type of disk. You can view the contents of a drive by clicking its icon in Windows Explorer or My Computer.

DRIVE LETTER

The naming convention for disk drives on IBM and compatible computers. Drives are named by letter, beginning with A, followed by a colon.

FILE

One or more items of similar data uniquely identified. A collection of records.

FILE TYPE

In the Windows environment, a designation of the operational or structural characteristics of a file. The file type identifies the program, such as Microsoft Word, that is used to open the file. File types are associated with a file name extension. For example, files that have the .txt or .log extension are of the Text Document type and can be opened using any text editor.

FIRMWARE

Program stored in a computer's memory or Read Only Memory.

FONT

A graphic design applied to a collection of numbers, symbols, and characters. A font describes a certain typeface, along with other qualities such as size, spacing, and pitch.

GROUP

A subset of the network established by the network administrator, usually based on departmental organization or physical proximity in the network. File protection facilities allow read/write restrictions for files and folders for groups, users, and the entire network.

HARD COPY

Computer output printed on paper.

HARD DISK

Disk made of rigid material.

HARDWARE

Physical parts of the computer system.

HIGH RESOLUTION

Quality of a display system or printer capable of reproducing images of great detail accurately.

INITIALIZE

To reset a computer system to a beginning point before starting a task. Also used to format a blank disk.

INPUT/OUTPUT

The transfer of information between a user and/ and or peripheral devices, files and the CPU.

INTERFACE

Device or program that allows separate parts of a computer to work together.

INSTRUCTION

Single order or command within a program.

I/O

See Input/Output.

LIBRARY

Collection of programs or data files.

LOG OFF

To sign off of the network.

LOG ON

To sign on to the network.

MEMORY

Part of a computer CPU that is able to retain binary coded information and instructions.

MENU

Program function options or choices displayed for user selection.

MICROPROCESSOR

CPU of a microcomputer.

MODEM

MOdulator-DEModulator. Peripheral used to interface a digital device with a telephone line, while encoding and decoding sequential bits of information into tone variations. Used for transmitting and receiving data.

NETWORK

Provides the capability for a number of computer systems and devices that are logically linked together to share resources by communicating with each other via telecommunications.

NETWORK ADMINISTRATOR

The person charged with planning, designing, and maintaining the network operation.

NODE

A computer or other device that is a member of the network.

ONLINE

Being connected to a computer system via telecommunications.

OPERATING SOFTWARE

Software program for an operating system.

OPERATING SYSTEM

Program that controls the execution of other programs, or software, within a computer system, and interprets application software commands.

OWNER

The person who "owns" a file. You are the owner of files you create.

PERIPHERAL

Accessory part of a computer system not essential to its operation.

PORT

Connecting point for joining hardware and peripherals to computer system.

POWER SURGE EQUIPMENT

Device that protects computer systems from power fluctuations, which may cause errors or a crash.

PROGRAM

Sequence of specified instructions that tells the computer what to do.

RAM

Random Access Memory. Temporary memory on chips, disk, or similar device. Data is used by the CPU and may be altered by the user. Information in a RAM chip is lost when power to the computer system is turned off.

READ/WRITE MEMORY

Alternate name for RAM.

ROM

Read Only Memory. Permanent memory included in a CPU that cannot be altered by a user or a program. Data in this memory is used by the CPU as soon as power is supplied to the computer system, in order to allow the system to be booted.

SCROLLING

Moving the information displayed on a screen up or down by one or more lines.

SOFTWARE

Computer programs; generally input on disk to a computer system.

USER-FRIENDLY

Capable of use by non-programming, or "user," personnel.

USERNAME

The name of the user that is typed to log on to the network.

WORK STATION

A stand-alone microcomputer or a terminal or microcomputer attached to a host computer.

General Keyboard Shortcuts

Press	To
CTRL+C	Copy.
CTRL+X	Cut.
CTRL+V	Paste.
CTRL+Z	Undo.
DELETE	Delete.
SHIFT+DELETE	Delete selected item permanently without placing the item in the Recycle Bin.
CTRL while dragging an item	Copy selected item.
CTRL+SHIFT while dragging an item	Create shortcut to selected item.
F2	Rename selected item.
CTRL+RIGHT ARROW	Move the insertion point to the beginning of the next word.
CTRL+LEFT ARROW	Move the insertion point to the beginning of the previous word.
CTRL+DOWN ARROW	Move the insertion point to the beginning of the next paragraph.
CTRL+UP ARROW	Move the insertion point to the beginning of the previous paragraph.
CTRL+SHIFT with any of the arrow keys	Highlight a block of text.
SHIFT with any of the arrow keys	Select more than one item in a window or on the desktop, or select text within a document.
CTRL+A	Select all.
F3	Search for a file or folder.
ALT+ENTER	View properties for the selected item.
ALT+F4	Close the active item, or quit the active program.
ALT+Enter	Displays the properties of the selected object.
ALT+SPACEBAR	Opens the shortcut menu for the active window.
CTRL+F4	Close the active document in programs that allow you to have multiple documents open simultaneously.
ALT+TAB	Switch between open items.
ALT+ESC	Cycle through items in the order they were opened.
F6	Cycle through screen elements in a window or on the desktop.
F4	Display the Address bar list in My Computer or Windows Explorer.
SHIFT+F10	Display the shortcut menu for the selected item.
ALT+SPACEBAR	Display the System menu for the active window.

CTRL+ESC	Display the Start menu.
ALT+Underlined letter in a menu name	Display the corresponding menu.
Underlined letter in a command name on an open menu	Carry out the corresponding command.
F10	Activate the menu bar in the active program.
RIGHT ARROW	Open the next menu to the right, or open a submenu.
LEFT ARROW	Open the next menu to the left, or close a submenu.
F5	Refresh the active window.
BACKSPACE	View the folder one level up in My Computer or Windows Explorer.
ESC	Cancel the current task.
SHIFT when you insert a CD into the CD-ROM drive	Prevent the CD from automatically playing.

APPENDIX D – END OF MONTH (SYSTEM ADMINISTRATION)

The following information is provided for System Administration purposes with the End of Month processes.

Daily Maintenance Procedures

1. System Administrator - Review End of Day logs each day through the Schedule Job Administration application. The system administrator or personnel responsible for monitoring end of day will invoke the Schedule Job Administration Application and the WIC Schedule Job Administration Applications and view the End of Day logs for potential errors that may need to be resolved before End of Day can process for the following day. In rare circumstances where End of Day is ended by user interaction or power surge
2. WIC Banking – You can access the <https://dataimagegateway.com> web site for Arkansas information. The system administrator responsible for bank transactions can access this site and view the bank transactions daily. Username and Password are required.

Monthly

Month End consists of two primary components: 1) Desktop Scheduling and 2) Month End Processing.

Desktop Scheduling

Scheduled Job Administration

Month End is scheduled using the Scheduled Jobs Administration interface.



Figure 1 – Scheduled Job Administration Main Window

To invoke WIC Month End Administration, click on the Scheduled Jobs option, WIC Month End Administration and select Run.

WIC Month End Administration

The WIC Month End Administration interface provides for adding and removing Month End from the schedule and the options to view or purge the Month End log. Also displayed are the latest Month End settings. The Month End Settings are helpful in understanding the system issued messages when attempting to add or remove from the schedule. For example, if the last status shows errors, then the user can expect to be guided by the system via messages when they select Add to Schedule. The messages will give options for restarting based on Month End settings and data.

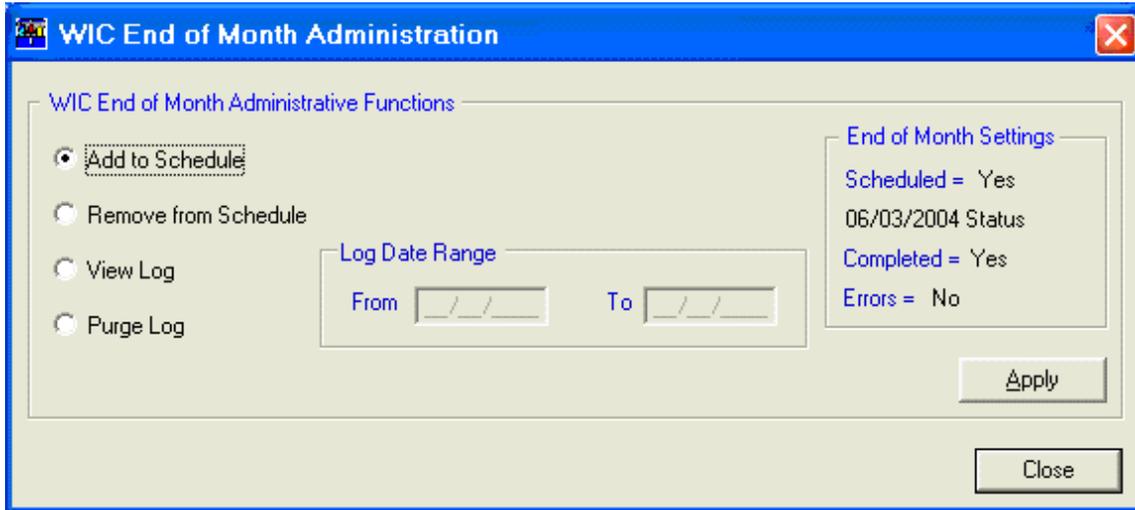


Figure 2 - WIC Month End Administration Main Window

Add to Schedule

To schedule Month End, select option Add to Schedule. Upon selection of Add to Schedule, pre-schedule validation occurs that involves:

1. Confirmation that Month End is currently not executing. If it is currently running, a message will be issued.
2. Verifies Bank Reconciliation totals. A state business rule is used to determine if this process is applicable to the state. If it is applicable and the bank totals do not reconcile, a text file is displayed with the bank totals. Month End cannot be scheduled until they have been corrected.
3. Determines the state/status of Month End. Each state/status is described below.

Month End State / Status

1. Normal Schedule:

The previous Month End executed successfully and the current month is ready to process. If the Month End status is determined to be a normal schedule, the following window will be displayed for confirmation to continue.

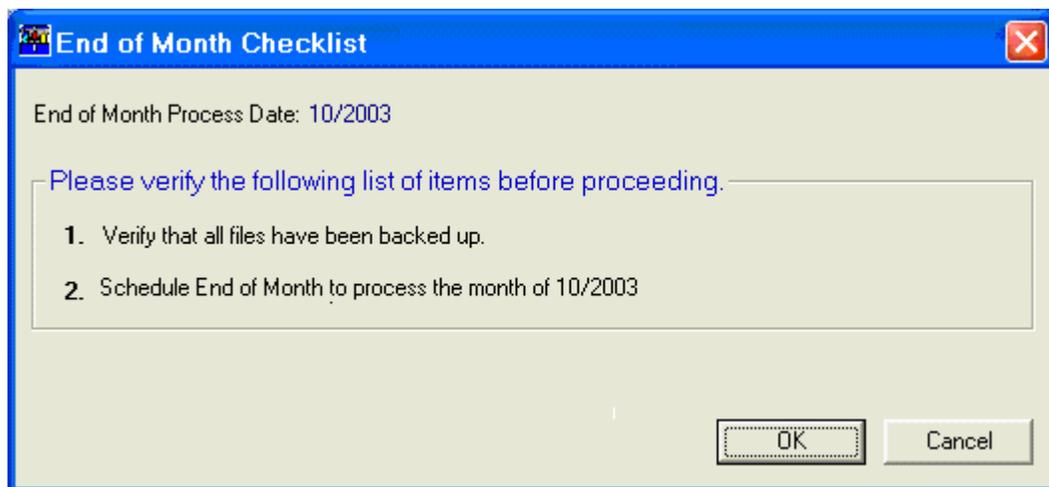


Figure 3 – Month End Checklist

Upon selection of OK, Month End will be scheduled to run.

- ◆ The exact time is dependent on when the daily schedule begins. If Month End is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ The Month End Settings will be changed to show Scheduled = Yes.

Restart Mode:

The current month end completed with errors. The Month End Settings, Errors = Yes, is indication that the state of Month End is restart mode. The Month End administrator would have received email notification from the Scheduled Job utility named Interrogator, that there was an error while processing Month End.

All errors will need to be researched and analyzed by technical support before attempting to add to Schedule. To assist in the understanding of the error, review the log to determine which processes completed successfully and those that completed with errors.

There are two types of restart a) Required Process Restart and b) Optional Process Restart.

Restart Type - Required Process

A required process did not complete successfully. The current month end must be restarted and allowed to complete all required processes. No additional Month End processing is allowed until this situation is resolved. It is recommended that you view the log prior to proceeding to determine which processes are affected by the restart.

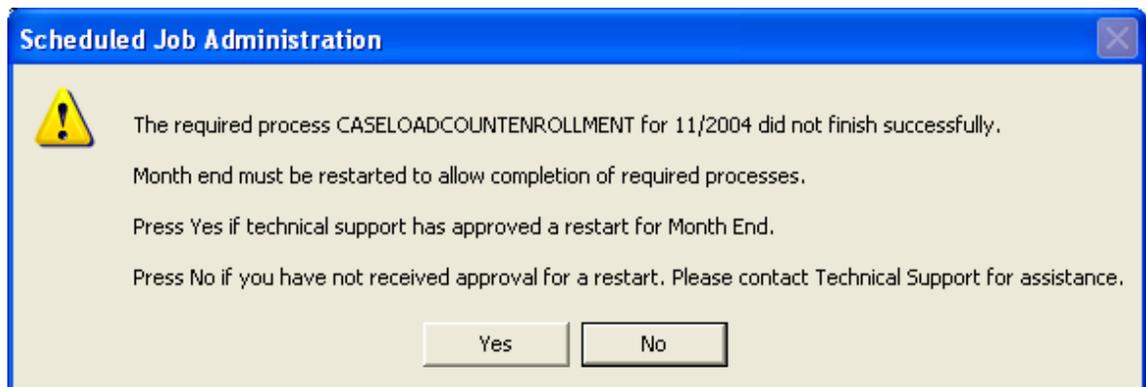


Figure 4 – Required Process Restart Message

Press Yes if technical support has given approval to proceed.

- ◆ Figure 3, Month End Checklist, will display for user confirmation. When confirmed, Month End will be scheduled to restart beginning with the process displayed.
- ◆ Any processes prior to the displayed process will not be processed again since they have successfully completed. Any process that follows the displayed process will run once the restarted process has completed successfully.
- ◆ If the restart is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ The Month End Settings will be changed to show Scheduled = Yes.

Press No if you are unsure that the issues have been resolved and want to cancel the restart.

Restart Type – Optional Process

An optional process did not complete successfully. When an error occurs with an optional process, all processes that follow the displayed process are allowed to continue. Month End always restarts with the first optional process that failed. If more than one optional process failed, they will also be restarted.

It is recommended that the log be viewed before making a decision. The processing order and where the displayed process is sequenced should be considered before restarting. For example, if the displayed process was the first optional process and the only process to fail, then it may be preferable to run the displayed process on demand rather than restarting Month End. Restarting will rerun the displayed process and all processes that follow in the processing order.

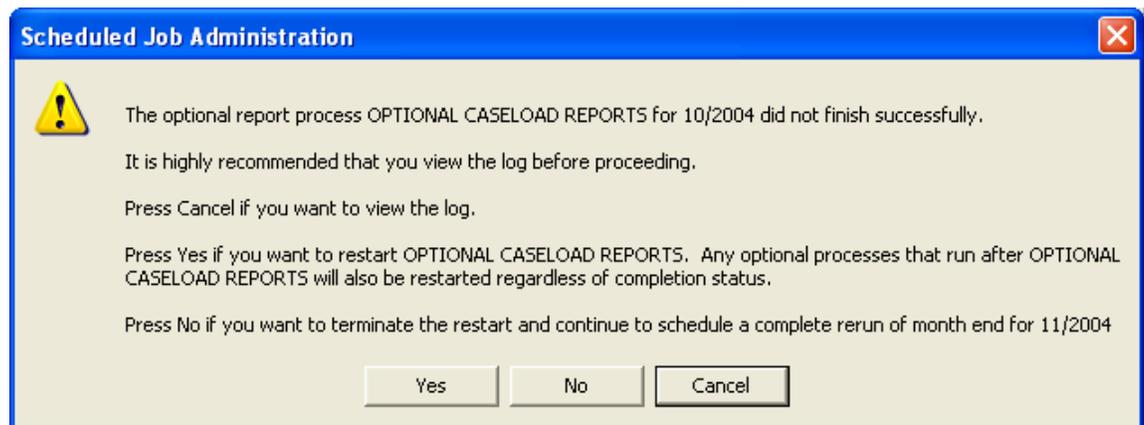


Figure 5 – Optional Process Restart Message

Press Yes to schedule Month End restart beginning at the displayed optional process going forward.

- ◆ Figure 3, Month End Checklist, will display for user confirmation.
- ◆ If the restart is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ A restart for an optional process is only applicable for the current month. If the restart is delayed until the next month end processing, the above message will not be displayed and a normal month end will be scheduled as described above for Normal Schedule. The optional processes will need to be run on demand if this situation occurs.

Press No to ignore the restart and to schedule a complete rerun of Month End for the current month.

- ◆ Figure 3, Month End Checklist, will display for user confirmation.
- ◆ If the rerun is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ Figure 6, Rerun Current Month End, will display for user confirmation to rerun.

Press Cancel for no action at this time.

Remove from Schedule

To remove Month End from the schedule, select option Remove from Schedule as shown on Figure 2 - WIC Month End Administration Main Window. Upon selection of Remove from Schedule, the system will verify that Month End is not currently running. If it is not running, then Month End will be removed from the schedule.

Month End is removed automatically from the schedule each time it runs with or without errors. The Month End Settings will generally show Scheduled = No. Use this option if you Add to Schedule and then must remove from the schedule before Month End actually runs.

Note: If the Month End scheduled was a restart or rerun, Remove from Schedule will reset Month End settings to the original values. The restart or rerun must be rescheduled by selecting Add to Schedule. The restart or rerun messages, whichever is applicable, will display again.

View Log

To view the Month End Log, select option View Log as shown on Figure 2 - WIC Month End Administration Main Window. A “From Date” and “To Date” range is required.

The Month End process that runs on the server logs an entry prior to each process. When possible, error messages are also logged. The Add to Schedule and the Remove from Schedule also writes entries to this log.

Purge Log

To purge the Month End Log, select option Purge Log as shown on Figure 2 - WIC Month End Administration Main Window. A “From Date” and “To Date” range is required.

It is recommended that you periodically purge data from the Month End log.

Month End Processing

The main processing for Month End was designed to run on a server. The application interface does not require interaction from a user. However, there are two exceptions that will require acknowledgement. 1) If the application is started again while it is currently running a message will be issued stating that another instance of the application is already running. 2) If the database table Currently_Executing shows a process that is in conflict with Month End a message will be displayed. The message will display the process name that conflicts with Month End.

The Month End administrator controls when Month End will execute using Desktop Scheduling as described in Section 1 of this document. When the administrator adds Month End to the schedule, the database table Scheduled_Job_Control is updated indicating that Month End is scheduled. This does not actually invoke Month End to run. Month End must be on an automated scheduler or manually invoked. When invoked, Month End reads Scheduled_Job_Control as the first step before proceeding. If the table indicates scheduled, then processing continues; otherwise, Month End immediately terminates successfully. This feature provides for the flexibility of keeping Month End on an automated scheduler to run each day without the need to alter the schedule. It is the Scheduled_Job_Control table maintained by the Month End administrator that determines when the processing actually takes place for the month.

Month End is automatically removed from the schedule by the Scheduled Job utility, Interrogator. It is always removed regardless if it completed successfully or completed with errors. Interrogator notifies the Month End administrator via email of the completion status.

If there are errors, the Month End administrator will need to work with technical support to correct the data before attempting to add month end to the schedule. In all cases, normal schedule, rerun and restart, the Month End administrator must use WIC Month End Administration, Add to Schedule to schedule Month End.

The Month End processing consists of required and optional processes. State business rules control which processes are applicable to the state. Only the processes applicable to the state will be executed.

The End of Month Processing includes:

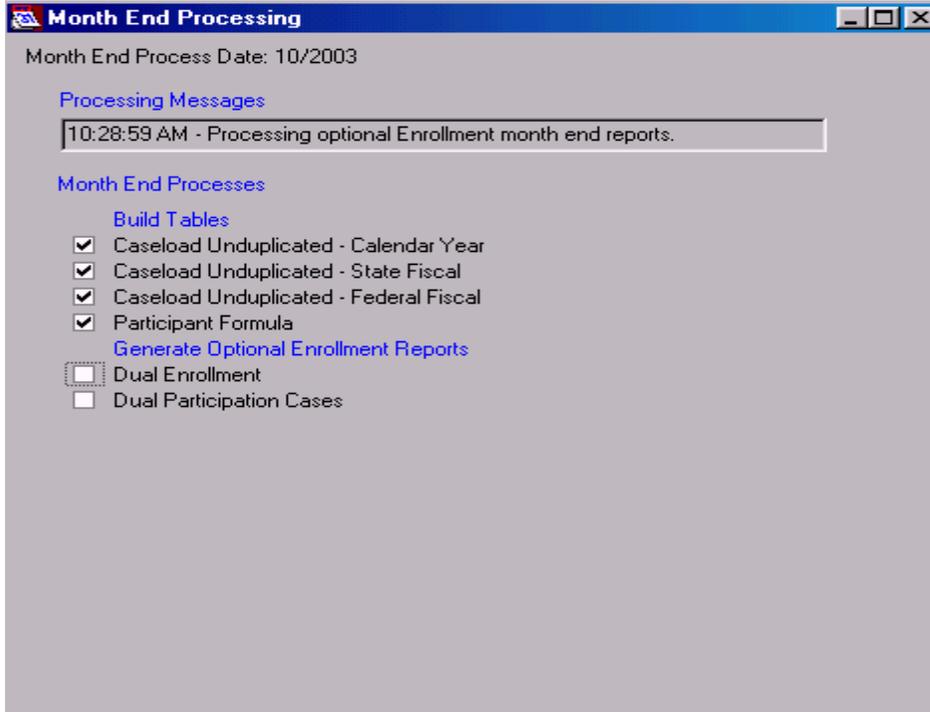
1. Rolling the Process Control Table Dates
2. Build Tables
 - Reported Participation Data
 - Enrollment Participation Data
 - Rebate Items
 - Vendor High Risk
 - Caseload Unduplicated - Calendar Year
 - Caseload Unduplicated - State Fiscal
 - Caseload Unduplicated - Federal Fiscal
 - Dual Enrollment - Enrolled and Participation
 - Participant Formula
 - Caseload Management Projection
 - FI Redemption Reconciliation
3. Generate Financial Reports
 - WIC Food Obligations and Expenditures
 - Average Cost Per Food Instrument Type
 - Food Instrument Redemption Summary
 - Food Instruments Redeemed Early
 - Food Instruments Redeemed Late
 - Supplier Rebate
 - Obligation Value for Outstanding FIs Issued
 - FMNP Food Expenditures
4. Generate High Risk Reports
 - Food Instruments Redeemed within \$5.00 of the Maximum Allowed Report
 - Food Instruments Redeemed within 85% of the Maximum Allowed Report
 - Vendors Whose Food Average Package Cost is More Than 10% Above Peer Group Average Report
 - Percent of Increase in Food Instruments Over Previous Month's Redemptions Report
5. Create Files
 - Create CDC Pregnancy File
 - Create CDC Pediatric File
 - Create External Dual Participation File for Oklahoma
6. Generate Optional Caseload Reports
 - Redeemed Participation Monthly
 - Reported Participation Monthly
 - Reported Participant High-Risk Outreach
 - Redeemed Food Instruments/Expenditures
 - Participation Processing Statistics
 - Enrollment Monthly
 - Unduplicated Enrollment-Yearly (Calendar Year)
 - Unduplicated Enrollment-Yearly (State Fiscal Year)
 - Unduplicated Enrollment-Yearly (Federal Fiscal Year)
 - Enrollment Unduplicated – Yearly

- Reported Participation Unduplicated – Yearly
 - Redeemed Participation Unduplicated – Yearly
 - Redeemed Participation Priority Summary
 - Redeemed Participation High Risk Priority Goal
 - Estimated Eligible Comparison Reported Participation
 - Enrollees by Age and Race/Ethnicity
 - Caseload Management Projection System Report
 - Food Instrument Package Cost
7. Generate Optional Nutrition Reports
 - Formula Compliance
 8. Generate Optional Enrollment Reports
 - Dual Enrollment
 - Dual Participation Cases
 9. Generate Optional Food Instrument Reports
 - List of Items Paid Without Issuance
 - Voided/Stolen and Cashed Exceptions
 10. Generate Optional Operation Reports
 - Migrant Enrollment
 - Non-Participation Reason by Category
 - Formula Supplementation of Breastfed Infants
 - Breastfeeding Certification Periods
 - Food Prescriptions
 - Special Formula
 - Participant Insurance Type
 - Medicaid Adjunctive Eligibility
 11. Generate Optional Financial Reports
 - Food Instruments Rejected for Payment
 12. Generate Optional Vendor Reports
 - High Cost Vendor Summary by Food Instrument Type
 - High Cost Vendor Summary by Vendor
 - High Cost Food Instrument Report
 - Low Variance Vendor Summary
 - Large Number of FI Rdmd Outside of Area
 - Redemption Twenty Percent Change
 - Small Volume Vendors < Than 25 Participants per Month
 13. Log Progress to the End of Month Log File

The following is a list of the required processes available in End of Month. As noted, there is a state business rule for each process so all processes may not be applicable to the state. The names shown below are used in user display messages and log messages.

CASELOAD COUNT
CASELOAD ENROLLMENT
CASELOAD REBATEITEMS
VENDOR HIGHRISK DATA
CASELOAD COUNT UNDUP
DUAL ENROLLMENT

PARTICIPANT FORMULA
REDEMPTION RECONCILIATION
CASELOAD PROJECTION
CDC FILES
EXTERNAL DUAL PARTICIPATION FILE
FINANCIAL REPORTS
HIGH RISK REPORTS



The following is a list of the optional processes available in End of Month. As noted, there is a state business rule for each process so all processes may not be applicable for your state. The names shown below are used in user display messages and log messages.

OPTIONAL CASELOAD REPORTS
OPTIONAL NUTRITION REPORTS
OPTIONAL ENROLLMENT REPORTS
OPTIONAL FOOD INSTRUMENT REPORTS
OPTIONAL OPERATION REPORTS
OPTIONAL FINANCIAL REPORTS
OPTIONAL VENDOR REPORTS

APPENDIX E – END OF DAY (SYSTEM ADMINISTRATION)

The following information will discuss the functions of the End of Day Process application that is run either manually or automatically on the Server at the end of the business day. The main processing for End of Day is designed to run on a server. The application interface does not require interaction from a user.

However, there are two exceptions that will require acknowledgement.

- 1) If the application is started again while it is currently running a message will be issued stating that another instance of the application is already running.
- 2) If the database table Currently_Executing shows a process that is in conflict with End of Day a message will be displayed. The message will display the process name that conflicts with End of Day.

For example, the End of Month processes use bank paid/rejected information for food instruments, which End of Day processes. Therefore the two processes must not run simultaneously.

The End of Day administrator controls when End of Day will execute using Schedule Job Administration (Chapter 09) and Windows Task Scheduler. When the administrator adds End of Day to the schedule, the database table Scheduled_Job_Control is updated indicating that End of Day is scheduled. This does not actually invoke End of Day to run. End of Day must be scheduled through Window Task Scheduler or some other form of automated scheduler or manually invoked. When invoked, End of Day reads Scheduled_Job_Control as the first step before proceeding. If the table indicates scheduled, then processing continues; otherwise, End of Day immediately terminates successfully. This feature provides for the flexibility of keeping End of Day on an automated scheduler to run each day without the need to alter the schedule. It is the Scheduled_Job_Control table maintained by the End of Day administrator that determines when the processing actually takes place for the month.

The End of Day Dialog will be initially displayed in a minimized state. The End of Day window can be restored by double clicking the title bar. A progress bar is displayed while the processes are running. All informative and error condition messages are saved to the End of Day event log. The processes run during End of Day are determined by the values that are set for each State Business Rule.

Log On

When End of Day Process is started, it will log into the system using a known username and password. This will give the program access to the database tables it needs to get the required information. The user name and password will come out of the registry from the server where End of Day is run:

```
HKEY_LOCAL_MACHINE\SOFTWARE\PDA\<STATE>VENDOR\COMMON\OBJECT  
OWNER.
```

The service name will be taken out of the registry on the server where End of Day is run: HKEY_LOCAL_MACHINE\SOFTWARE\ PDA \<STATE>VENDOR\COMMON\SQLSERVERDBSERVICE.

Progress Meter

When the End of Day dialog is restored (not minimized), the progress meter is displayed to inform the user of End of Day processing status. The progress meter displays the percentage complete for the processing of the files. Once the meter reaches 100% the End of Day process is complete.



Figure 1– End of Day Dialog

Controls

End of Day Percent Complete Progress Bar

This control displays a progress indicator for the End of Day process.

Characteristics

The progress bar will be enabled when the form is active. It will display, in a graphical display, the percentage of completion.

Validation of Required Settings Logged messages

This section describes the processes (navigation) that take place as a result of the actions taken on the End of Day Conflicts.

System Registry Entries

If the system registry has been updated or corrupted, a system message is written to the log file with the message text, "The system was unable to retrieve the end of month reports file folder name from the registry. Please contact technical support for assistance."

If the required registry entry for End of Day is not found in the Windows System Registry, End of Day Processing will be terminated. A message box will be written to the log file with the message text "A directory or file defined in the Registry for the End of Day process does not exist".

Order of processing

The order of processing end of day will be determined by the value in the State Business Rules entity and if applicable for your state. Processes, imports and exports applicable for your state will be processed. Processes are run first, imports second, and exports last.

Process Sanction Points

Sanction points that no longer apply will be 'rolled-off' the system. The sanction points accumulate over the lifetime of the Vendor contract. These sanction points may no longer be counted against a vendor after a period of time. Each violation has a different expiration date that varies from 0 days to infinite. The End of Day Process will roll-off the expired sanction points that meet certain criteria. This process is applicable for your state if the State Business Rule EOD_PROCESSSANCTIONPOINTS = 'Y'.

Roll-off points

If EOD_PROCESSSANCTIONPOINTS = 'Y' in the StateBusiness rules table, all Sanction points in the Violation table with an ApplyUpTo date greater than the EODLastRunDate in the System Information table and less than or equal to the current system date will be gathered and subtracted from the parent records in the FollowUpActivity table and the Event table.

Process Pending Disqualification

The End of Day process will change a vendor to a Disqualified status if the vendor grace period has expired and the vendor is in a Pending Disqualification status. This process is applicable for your state if the State Business Rule EOD_PROCESSPENDINGDISQUALIFICATION = 'Y'.

Process Pending Disqualifications

If EOD_PROCESSPENDINGDISQUALIFICATION = 'Y' and the TerminationDate in the TermDisqualification table is greater than the EODLastRunDate in the SystemInformationtable and less than or equal to the current system date, the system will change the Vendor from a Pending Disqualification status to a Disqualification status. The system will calculate the ReinstatementDate for the vendor. The ReinstatementDate is calculated by adding the DaysDisqualified in the TermDisqualification table to the current system date for the applicable record. If more than one record exists, the most recent record is applied. The calculated date is added to the ReinstatementDate field in the Vendor table for the associated vendor record.

Process Peer Group Pricing

The End of Day process has two essential ways to determine the maximum prices. Firstly, it can calculate the Max Peer Group Pricing based on actual redemption information by examining a 3-month rolling average of Food Instrument data. The second option is to evaluate the Vendor's surveyed prices for food items across their peer groups. Which option End of Day runs depends on the value of the State Business Rule EOD_3MONTHROLLINGAVG.

There is an additional State Business Rule EOD_COSTCONTAINMENTONLYUSES3MONTHAVG that can be turned on that will allow End of Day to calculate the Non Over 50% Vendors peer group max price by using the surveyed prices method and calculate the Over 50% Vendors peer groups using the 3 Month Rolling Average method.

Process 3 Month Rolling Average for Peer Group Pricing

An End of Day process will recalculate the peer group average and maximum prices every 2 weeks based upon actual redemption to obtain a 3-month (12 week) rolling average for the peer group food instrument type or food item. This process is applicable for your state if the State Business Rule EOD_3MONTHROLLINGAVG = 'Y'.

The manually calculated average price for each food item is needed for state office obligations, reporting and rebates when paper FIs are issued. It will replace the manually calculated Average and Maximum Prices for the Food Instrument Type and Peer Group.

Process 3 Month Rolling Average

For Paper Food Instruments:

The system will calculate the 3-month rolling average every 2 weeks by selecting issued food instruments that have been redeemed over the last 12 weeks. It will calculate the average redemption amount (the mean) within each food instrument type and vendor peer group combination and update the AvgPrice column in the PEERGROUPFOODINSTTYPEPRICE table. For each vendor peer group and food instrument type it will determine the standard deviation value (the mean of the mean) and increase the maximum price by the value set for the

EOD_3MONTH_ROLLING_AVG_NBR_STD_DEVIATIONS business rule to determine the standard deviation. This information is stored in the Price column of the PEERGROUPOODINSTTYPEPRICE table.

Process Reinstate Vendor and Vendor Stamp

The end of day process will reinstate vendors and vendor stamps

Reinstate Vendor and Vendor Stamp

The system will update all vendors, if the Reinsate.ReinstateDate is <= the current system date and the Reinsate.UpdateRecord = 'U'. The end of day process will set the Vendor.CurrentStatus = '3' (enrolled). The system will update the StatusHistory table with the change in vendor status information.

If the ReinstateVendorStamp flag = 'Y', the system will update the VendorStampHistory with the change in stamp information. The system will remove the vendor from the TermDisqualification table. The system will remove the DeactBankEffective date from the TerminateStamp table for the reinstated stamp number for the primary vendor stamp number (Vendor.StampNumber). The system will set the Reinsate.UpdateRecord = 'N' for the VendorID

Adjust/Archive/Purge Process

The End of Day process will change (or move) a participant to Agency '88' when the participant is no longer eligible for WIC. This process is applicable for your state if the State Business Rule EOD_PROCESSADJUSTMENTSHIDES = 'Y'.

Process Adjust Records

If EOD_PROCESSADJUSTMENTSHIDES = 'Y', the system will update Member records to the appropriate status depending on the following criteria.

ADJUST RULES FOR EOD	ACTION
Child records over the Age defined in the State Business Rule. <i>MaximumChildAge</i> and not in a valid certification process.	Change to Categorically Ineligible
Women over the Age defined in the State Business Rule. <i>MaximumWomanAge</i> and not in a valid certification process.	Change to Categorically Ineligible

<p>Participants who have been certified for more for more days than the value of the <i>CertLimitWithPendingIDProof</i> business rule without Proof of ID will be marked as terminated. Homeless participants are excluded from this process.</p> <p>If the participant is an Infant or a Child, this is determined by validating the Member.IdentificationProof value = ‘PendingIDProofValueChild’ business rule and the current system date is greater than the <i>CertLimitWithPendingIDProof</i> business rule and Household.Homeless value is ‘N’ or null.</p> <p>or</p> <p>If the participant is a Woman, this is determined by validating the Member.IdentificationProof value = ‘PendingIDProofValueWoman’ business rule and the current system date is greater than the <i>CertLimitWithPendingIDProof</i> business rule and Household.Homeless value is ‘N’ or null.</p>	<p>Mark as terminated</p>
<p>Participants who have been certified for more days than the value of the <i>CertLimitWithPendingResidencyProof</i> business rule without Proof of Residency will be marked as terminated. Homeless participants are excluded from this process</p> <p>For all WIC Categories, this is determined by validating the Member.ResidencyProof value = ‘PendingResidencyProofValue’ business rule and the current system date is greater than the <i>CertLimitWithPendingResidencyProof</i> business rule and Household.Homeless value is ‘N’ or null.</p>	<p>Mark as terminated</p>
<p>Participants who have been certified with pending proof of income eligibility for more days than the value of the <i>CertLimitWithPendingIncomeProof</i> business rule without additional income information that includes a proof of income.</p> <p>For all WIC Categories, this is determined by validating the IncomeContact.PendingProof value = ‘Y’ and the current system date is greater than the <i>CertLimitWithPendingIncomeProof</i> business rule.</p>	<p>Mark as terminated</p>
<p>Categorically ineligible participants.</p>	<p>Mark as terminated</p>
<p>Participants who have been certified with delayed blood for more days than the value of the <i>CertLimitWithDelayedBlood</i></p>	<p>Mark as terminated</p>

Participants who have failed to pick up food instruments for two consecutive months or have failed to re-certify for 31 days past their certification due date who are not in a new certification process	Mark as terminated
Participants who have been certified with risk factor 503 (Presumptive Eligibility) for more days than the value of the <i>CertLimitWithRF503NoHW</i> business rule without a height/weight measurement contact	Mark as terminated
Participants who have been certified with risk factor 503 (Presumptive Eligibility) for more days than the value of the <i>CertLimitWithRF503NoBlood</i> business rule without a blood work contact	Mark as terminated
Participant who have started a certification attempt but did not complete within the time allowed Adjust Certification Records: <ol style="list-style-type: none"> 1. Participants with a WICSTATUS of Pregnant (P) and a certification has been started but not completed within the number of days defined in the business rule <i>IncompCertLimitPregnant</i> from the certification start date, the participant's certification record is changed to ineligible. 2. Participants whose household record indicates he/she is a Migrant and a certification has been started but not completed within the number of days defined in the <i>IncompCertLimitMigrant</i> business rule from the certification start date, the participant's certification record is changed to ineligible. 3. All Participants with the exception of pregnant women and immigrants, if a certification has been started but not completed within the number of days in the <i>IncompCertLimitOther</i> business rule from the certification start date, the participant's certification record is changed to ineligible. 	Change certification to ineligible and queue Ineligibility notice
Infant to a child when the infant reaches his or her first birthday unless they are currently in a new certification attempt. A pseudo-certification record will be created for the child, and all applicable risk factors will be carried forward from infant to the child pseudo-certification record.	Change WIC Category from I to C
Synchronize the certification information in the Member table to the certification information in the CertContact table when the current certification start date is greater than the certification start date in the Member table.	Update the Member table with the CertContact information.

Update the Valid Certification flag when the participant is no longer in a valid certification	Update Valid Certification flag
Reset all On Premises times for the household members	Reset OnPremisesTime in Member Record

Process Archive Records

The End of Day Process automatically archives records by changing the Agency ID in the Member table to '88'. Agency '88' is used to indicate the member is archived from the active system and will not be visible to the user in the Service Site Application. The member is used for historical reporting, and is not used for current reporting.

ARCHIVE RULES FOR EOD	ACTION
Participants who have not been back for 60 days after applying for WIC	Move to agency '88'
Participant was terminated more than 6 months ago and has not been serviced and they are not currently in a new certification attempt.	Move to agency '88'
Participant whose last certification attempt was ineligible more than 6 months ago and has not been serviced.	Move to agency '88'

Process Purge Records

The End of Day Process automatically archives records by deleting them from the system database.

PURGE RULES FOR EOD	ACTION
Purge Household records that have no members	Delete Household record
Purge Event Logs older than 14 days.	Delete EventLog records
Purge Business Hours Older than 90 days	Call Appointment Scheduler Purge
Purge Appointments at least 3 months old	Call Appointment Scheduler Purge
Purge Class Enrollments older than 7 months	Call Appointment Scheduler Purge
Purge Group Education Classes older than 7 months	Call Appointment Scheduler Purge
Purge Holidays older than 90 days	Call Appointment Scheduler Purge

Send/Receive External Files Process (FTP)

If your state has both SPIRIT WIC application front-end and back-end system the End of Day process will run FTP processes to Send/Receive external files. This process is

applicable for your state if the State Business Rule EOD_SENDRECEIVEEXTERNALFILES = 'Y'. Refer to Chapter 07 - Send_Receive (FTP or Dialup) (EOD).doc for more information on this process.

Import Files

Files created for import to the SPIRIT WIC system are placed in the required directories by the SPIRIT WIC system, an external system or the user. Some files are received for the sole purpose of exchanging data with systems that do not have the SPIRIT WIC front-end applications. The function of moving, copying, backing up and archiving all import files is a manual function performed by the user. The SPIRIT WIC system will then import all files according to the State Business Rules. The registry key for the import file directory is HKEY_LOCAL_MACHINE\SOFTWARE\PDA\
<STATE>VENDOR\VendorEOD\ReceiveFromDirectory

Import Issuance File Process

The End of Day process will import Food Instrument Issuance data from an ASCII file format. This process is applicable for your state if the State Business Rule EOD_ISSUANCEFILEIMPORT = 'Y'.

Process Issuance File

If EOD_ISSUANCEFILEIMPORT = 'Y' and an Issuance file is located in the \\<STATECODE>EOD\ISSUANCE\ **directory**, the End of Day Process will Add/Update the Issuance data in the associated Food Instrument tables. Refer to Chapter 05 – Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout. If an import file is found then it will be processed, if not the process is bypassed. If multiple import files are found for a process then the import files will be processed in order from oldest to newest based on import file date and time stamp. Import files are renamed after processing so they will not be processed more than once.

Import Banking Paid File

The End of Day process will import Banking Paid data from an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGPAIDFILEIMPORT = 'Y'.

Process Banking Paid File

If EOD_BANKINGPAIDFILEIMPORT = 'Y' and a Banking Paid file is located in the \\<STATECODE>EOD\BANKING\ **directory**, the End of Day Process will Add/Update Food Instrument Paid/Rejected data in the associated Food Instrument tables. Refer to Chapter 05 – Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout. If an import file is found then it will be processed, if not the process is bypassed. If multiple import files are found for a process then the import files will be processed in order from oldest to newest based on import file date and time stamp. Import files are renamed after processing so they will not be processed more than once.

Import Food Instrument File

SOAP/XML import for the Food Instrument file is no longer applicable.

Export Files

The files created by the SPIRIT WIC system are placed in specific directories for the user to locate. Some files are generated for the sole purpose of exchanging data with systems that do not have the SPIRIT WIC front-end applications. The function of moving, copying, backing up and archiving all export files is a manual function performed by the user. The registry key for the export file directory is HKEY_LOCAL_MACHINE\SOFTWARE\PDA<STATE>VENDOR\VendorEOD\SendToDirectory.

Export Banking Price File

The End of Day process will export Peer Group Pricing data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGPRICEFILEEXPORT = 'Y'.

Create Banking Price File

If EOD_BANKINGPRICEFILEEXPORT = 'Y', the End of Day Process will export the Peer Group Food Instrument Type Price data to an ASCII flat file. The file naming convention is <STATECODE>BP#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking Stamp File

The End of Day process will export Vendor Stamp data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGSTAMPFILEEXPORT = 'Y'.

Create Banking Stamp File

If EOD_BANKINGSTAMPFILEEXPORT = 'Y', the End of Day Process will export the Vendor Stamp data to an ASCII flat file. The file naming convention is <STATECODE>BS#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking Vendor File

The End of Day process will export Vendor demographics data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGVENDORFILEEXPORT = 'Y'.

Create Banking Vendor File

If EOD_BANKINGVENDORFILEEXPORT = 'Y', the End of Day Process will export the Vendor demographics data to an ASCII flat file. The file naming convention is <STATECODE>BV#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking New FI Issuance File

The End of Day process will export New FI Issuance data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGISSUANCEFILEEXPORT = 'Y'.

Create Banking New FI Issuance File

If EOD_BANKINGISSUANCEFILEEXPORT = 'Y', the End of Day Process will export the New Food Instrument Issuance Bank data to an ASCII flat file. The file naming convention is <STATECODE>BI#####.TXT and is stored in the \\<STATECODE>EOD\BANKING. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking FI Stop Payment File

The End of Day process will export the FI Stop Payment data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGSTOPPAYFILEEXPORT = 'Y'.

Create Banking FI Stop Payment File

If EOD_BANKINGSTOPPAYMENTFILEEXPORT = 'Y', the End of Day Process will export the Food Instrument Stop Payment Bank data to an ASCII flat file. The file naming convention is <STATECODE>BY#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Vendor File

The End of Day process will export the Vendor demographics data to an XML file format using SOAP methods. This process is applicable for your state if the State Business Rule EOD_VENDORFILEEXPORT = 'Y'.

Create Vendor File

If EOD_VENDORFILEEXPORT = 'Y', the End of Day Process will export the Vendor Demographics data to an XML file. The file is stored in the \\<STATECODE>EOD\VENDOR\REQUEST directory. Refer to Chapter 06 - SOAP_XML Files (EOD).doc for specifics on the XML file layout.

Process CDC File

If a CDC file exists in the C:\WICCDCFiles\ Subfolders: Pediatric or Pregnancy, the End of Day process will submit the files as defined by the information listed in the COMMREQUEST table. If the SENDEMAIL value is 'Y' in the COMMREQUEST table then E-Mail will be sent along with the files to notify the CDC that the files were sent. If the SENDEMAIL value is "N" then the files are sent but no E-Mail notification is sent.

Calculations for computing 3 Month Rolling Average

Paper FIs Food Instrument Type Average and Maximum Price

Sum the paid amounts from FIs redeemed over the last twelve weeks (today minus twelve weeks).

Caveats: The goal is to cover all WIC approved food benefits issued on the FI. The clients are instructed to select least expensive items and the vendors are trained accordingly. At one standard deviation, the paper FI Type food items really need to be grouped on a single FI in a manner such that the items are habitually redeemed in full more often than not. At one standard deviation, if the 50% clients are consistently not redeeming the tuna at all and only part of the carrots and beans then it is possible that the maximum price could fall short for the client who redeems the full set of full food benefits on the FI. This grouping of food benefits on a single FI to support the max price at the bank will be covered in training.

We may need to provide a variable allowing the user to choose a 1, 2, or 3 standard deviations to apply. By mathematical convention, applying one standard deviation of its average, 68.3% of your dataset is generally included. At two standard deviations, 95.4% within plus/minus these two standard deviations of your average is generally included. At three standard deviations, 99.7% of your price data is generally included.

Calculation

Calculate Pricing:

Average Price = Mean Redemption Amount over twelve weeks

Maximum Price = Redemption Amount over twelve weeks plus one standard deviation

Normal Distribution of Data:

A normal distribution of data means that most of the examples in a set of data are close to the “average,” while relatively few examples tend to one extreme or the other.

Standard Deviation: A measure describing how close members of a data set are in relation to each other. The standard deviation is kind of the “mean of the mean” (average variance of an average), and often can help you find a pattern in the data. The standard deviation can be found by taking the square root of the variance. If the variance is 25, the standard deviation is 5.

Square Root: One of two equal factors of a given number. For example, 5 is a square root of 25 because $5*5 = 25$. Another square root of 25 is -5 because $(-5)*(-5) = 25$. The +5 is called the principle square root of 25.

Two Variance Methods:

- biased variance and standard deviation
- unbiased variance and standard deviation

Biased or Unbiased Variance Method:

For the Unbiased Method = Divide the result by the count of items in the set of data minus 1 item (standard variance value)

For the Biased Method = Divide the result by the count of items in the set of data (forcing a result of a lower variance value or a deviated variance)

The Unbiased Variance method provides a common deviation value. You should use the Unbiased Method, because it is the standard default method, unless there is a business reason to understand and use a deviated variance

In both variance method examples in the document, you begin with all three items in the data set count to produce the mean or average value.

To determine the Biased variance value, use the full count of the items in the dataset that were used to calculate the mean (average). Because the Biased Variance Method results in a lower variance value (a deviated rate below the standard variance), you do not reduce the dataset count by one.

Terms Used:

x = one value in the set of data
(the redeemed amount)

$avg(x)$ = the average of all the values x in your set of data, the mean

- Paper FIs: (the sum of the redeemed amounts for the last twelve weeks by peer group and food instrument type)
- n = the number of values (item count) in the set of data

Business Rules:

A State Business Rule defines the number of standard deviation to apply to the mean. If the State Business Rule EOD_3MONTH_ROLLING_AVG_NBR_STD_DEVIATIONS= '1' then one standard deviation is applied.

A State Business Rule defines the variance method use when calculating the standard deviation. If the State Business Rule EOD_3MONTH_ROLLING_AVG_VARIANCE_METHOD= 'B' then the biased variance method is applied.

Formula Used:

1. Count the number of items in the set of data for the beginning value of n.
2. Find the average value of all items in the set of data. Average Price = Mean Redemption Amount over twelve weeks
3. For each value x, subtract the overall avg (x) from each x. When result is negative it means that x is below the mean.
4. Multiply that result by itself (otherwise known as determining the square of that value). The result is positive.
5. Sum up all those positive squared values.
6. For the Biased Method = Divide that result by (n).
7. For the Unbiased Method = Divide that result by (n-1).
8. Find the square root of that last number, the variance, for the value of the standard deviation of your set of data. The standard deviation is the positive square root of the variance, the mean of the mean.
9. Maximum Price = Average Price plus one standard deviation.

For the data set example {1,2,3} there are a total of three items in the set of data, therefore the value of n begins at 3

1. n=3 for the total of three items in the set of data
2. $1+2+3 = 6$ for the total of the value of all items in the set of data
 $6 / 3 = 2$ to find the average value of the set of data
3. $1-2 = -1$; $2-2 = 0$; $3-2 = 1$
4. $-1 * -1 = 1$; $0 * 0 = 0$; $1 * 1 = 1$
5. $1 + 0 + 1 = 2$
6. Biased Method: $2 / 3 = .666666666$ or .667
7. Unbiased Method: $2 / 2 = 1$
8. Biased Method: the square root of .667 is .8168 rounded to 82 cents
Unbiased Method: the square root of 1 is 1
9. Biased Method: $2 + .82 = 2.82$ (**results in a lower variance value**)
Unbiased Method: $2 + 1 = 3$ (**results in a standard variance value**)

The **biased** variance is:

$$\frac{(1-2)^2 + (2-2)^2 + (3-2)^2}{(3)} = .666666666 \text{ or } .667$$

The standard deviation is the square root of the biased variance, which equals:

$$\sqrt{0.667} = .8168$$

The mean plus one standard deviation for the biased variance equals:
 $2 + .8168$

The **unbiased** variance is:

$$\frac{(1-2)^2 + (2-2)^2 + (3-2)^2}{(3-1)} = 1$$

The standard deviation is the square root of the unbiased variance, which equals:

$$\sqrt{1} = 1$$

The mean plus one standard deviation for the unbiased variance equals:
 $2 + 1$

Process 3 Month Rolling Average for Peer Group Pricing

An End of Day process will recalculate the peer group average and maximum prices every 2 weeks based upon actual redemption to obtain a 3-month (12 week) rolling average for the peer group food instrument type or food item. This process is applicable for your state if the State Business Rule EOD_3MONTHROLLINGAVG = 'Y'.

The manually calculated average price for each food item is needed for state office obligations, reporting and rebates when paper FIs are issued. It will replace the manually calculated Average and Maximum Prices for the Food Instrument Type and Peer Group.

Process 3 Month Rolling Average

For Paper Food Instruments:

The system will calculate the 3-month rolling average every 2 weeks by selecting issued food instruments that have been redeemed over the last 12 weeks. It will calculate the average redemption amount (the mean) within each food instrument type and vendor peer group combination and update the AvgPrice column in the PEERGROUPFOODINSTTYPEPRICE table. For each vendor peer group and food instrument type it will determine the standard deviation value (the mean of the mean) and increase the maximum price by the value of one standard deviation. This information is stored in the Price column of the PEERGROUPFOODINSTTYPEPRICE table.

APPENDIX F – ON-GOING MAINTENANCE, REPAIR AND REPLACEMENT OF ARKANSAS AGENCY EQUIPMENT

On-going Maintenance, Repair and Replacement of Arkansas agency equipment

Arkansas agencies are responsible to replace consumable items supporting on-going maintenance. (e.g. toner, paper, check stock, batteries needed for e-signature pads and mice). Each agency will provide their own removable storage media (e.g. CD-R, CD-RW, DVD-R, or USB removable storage media) for copying Microsoft Office files.

Arkansas has purchased a limited amount of spare equipment to be loaned to Arkansas agencies while agency equipment is being repaired. Agencies experiencing equipment problems should contact the ADH Help Desk immediately. The ADH Help Desk staff will identify equipment problems and fixes, coordinate warranty repairs, and be the point of contact to arrange for loaners (spare equipment) to be shipped to agencies while repairs are performed.

When new equipment needs arise, agencies are to contact the ADH Help Desk. The ADH Help Desk will provide equipment specifications, recommendations, and support to configure the new equipment for the SPIRIT application. All new equipment must comply with project equipment specifications.

APPENDIX G – SETUP PROCEDURES FOR DATA SYNC

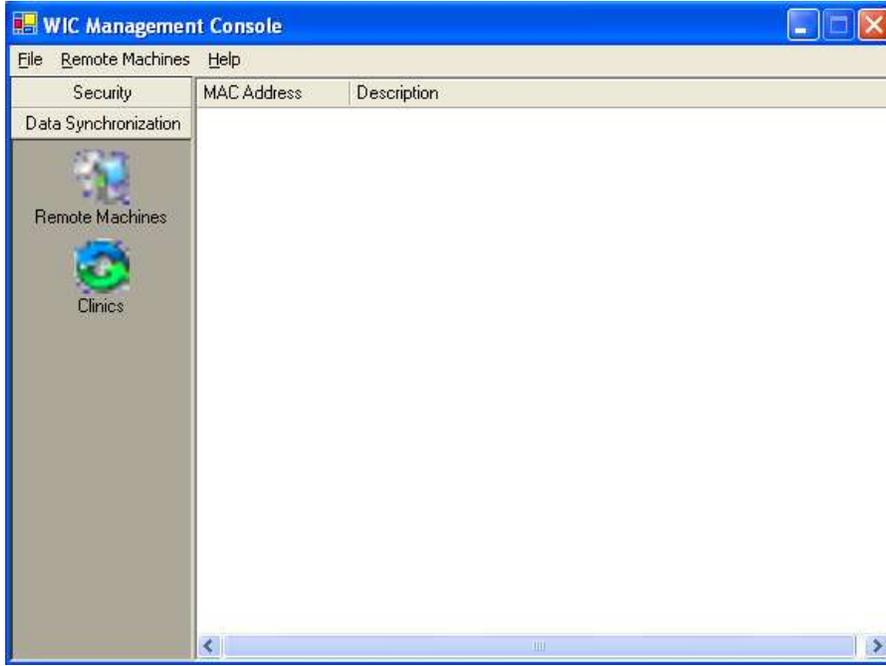
1) On the laptop setup a user called “spirit” in enterprise manager.



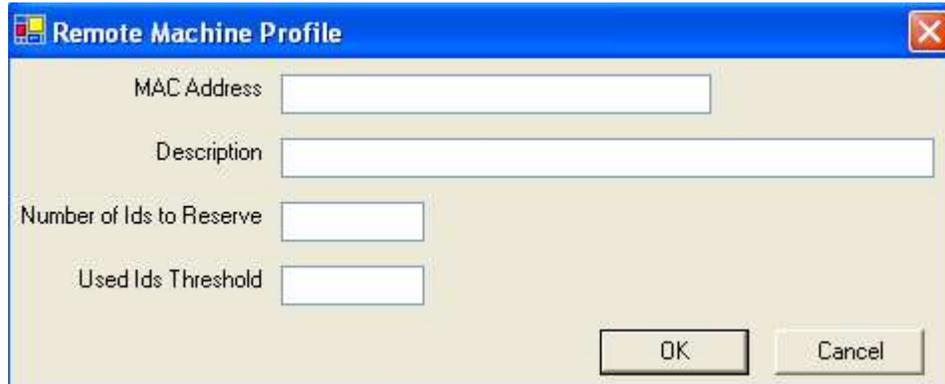
Make sure the username is set to “spirit” and the password is set to “sp1r1t76”. Also, check the System Administrators and Server Administrators boxes under the Server Roles tab.

2) Restore a backup of the production database to the laptop instance of SQL server.

3) Open Management Console and click on the Data Synchronization.



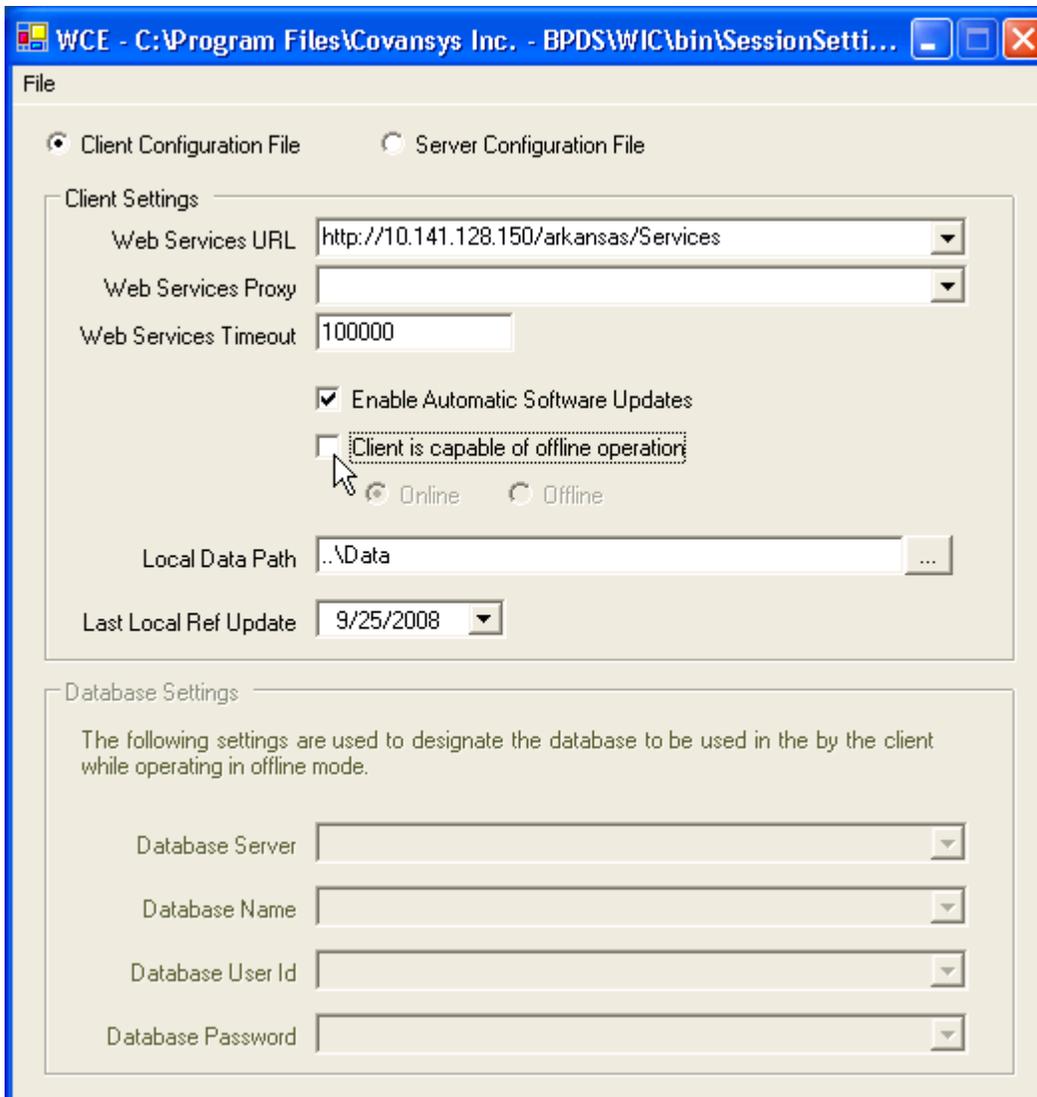
Now click on the Remote Machines button. This will change the menus. Click on the “Remote Machines” in the menu and select Add.



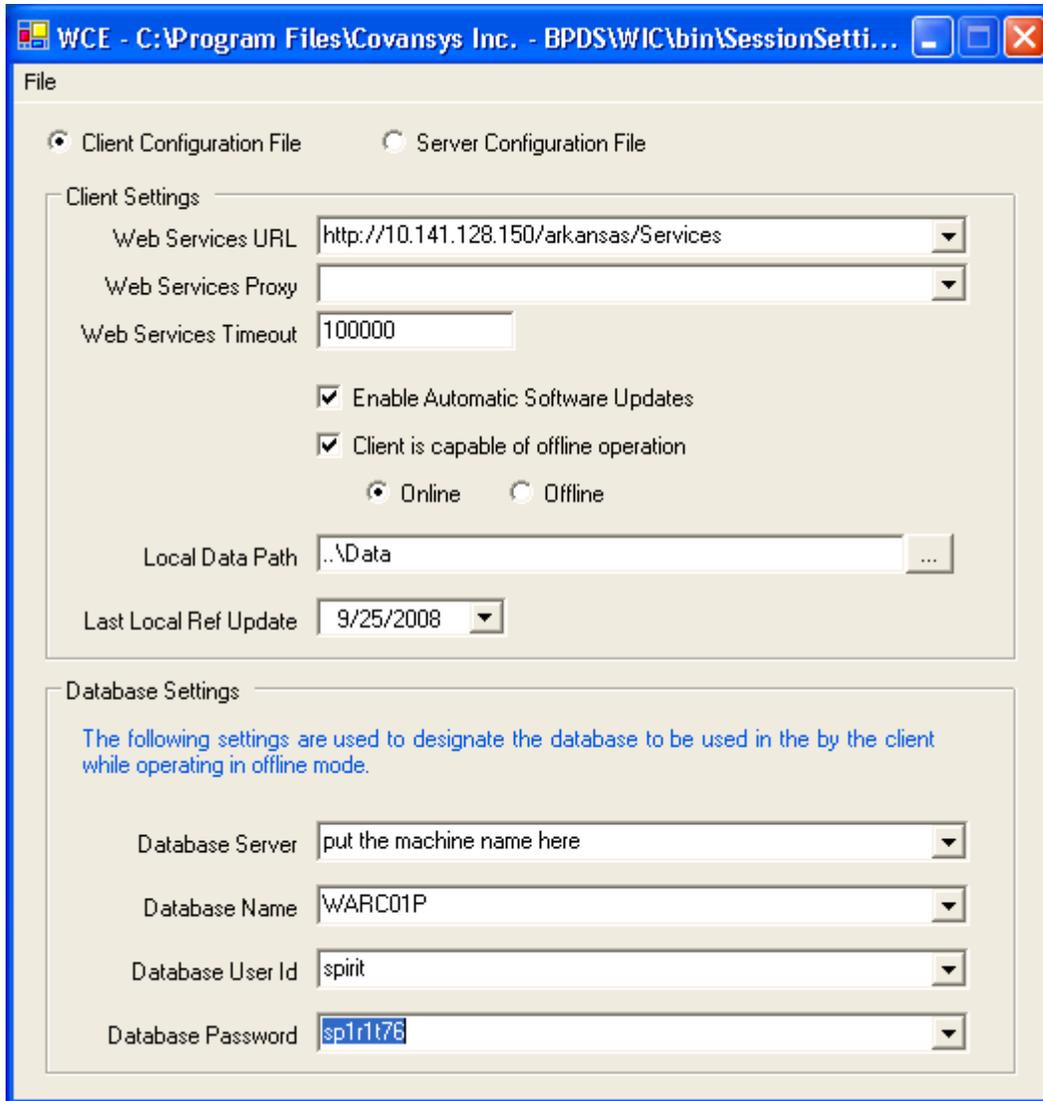
Enter the MAC address of the laptop that will perform the data sync. Note: There may be more than one MAC address. Use the appropriate address base on how the laptop is connected to the network. Next enter a Description for the laptop. Now enter the number of ID’s to be reserved for off line mode and the threshold. For the average clinic 500 ID’s should be reserved and 90 for the threshold

4) Setup the WIC config editor.

Click the WIC config editor icon. Once open select File and then open. The “SessionSettings.xml” should be in the file name. Next click Open.



Now check the “Client is capable of offline operation”



Next set the
 Database Server to the system name of the laptop
 Database Name to the appropriate name

Database Name	State
WARC01P	Arkansas Production

Database User Id to “spirit”
 Database Password to “sp1r1t76”
 Now click File-> save

5) Open the SessionSettings.xml file found in the C:\Program Files\Covansys Inc. - BPDS\WIC\bin directory. Establish the LastDataCheckoutAt date and time. It should roughly correspond to the date and time of the database backup. The Data Sync software uses this value to determine the cutoff time when bringing changes down. It will update this value after a successful checkout.

6) Now open the “Data Sync Client – Checkout” application on the laptop. Select the clinic to check out and click the check out clinic button. Once the check out is complete the data sync software will log the user off. The next time the user logs in they will be in the off line mode. i.e. checked out.

Arkansas WIC Program Blanket Purchase Agreements

Equipment Blanket Purchase Agreement

<http://www.dell.com/learn/us/en/84/slg/arkansas?c=us&l=en&s=slg&cs=84>

Services Blanket Purchase Agreement

<http://www.dfa.arkansas.gov/offices/procurement/contracts/Pages/default.aspx>

Software Purchase Agreement

<http://www.dfa.arkansas.gov/offices/procurement/contracts/Pages/wscSoftware.aspx>

Risk Assessment and Control Activities Worksheet

Agency: Arkansas Department of Health
 Department: Administration
 Activity: Information Technology Services

Prepared By: Michael Kincaid
 Date Prepared: March 20, 2014

Objective Type	Objectives	Risk Assessment			Actions to Manage Risks		Mgmt Conclusion	Corrective Action Plan
		Risks	Significance / Impact	Likelihood	Control Activities	New or Additional Control Activity		
(O)	IT	Inadequate system design and development	Moderate	Low	Training on .net and SQL 2008	S	Sent 2 System engineers to training on SQL Server 2012 platform since last Risk Assessment was completed in 2013.	
(O)		Hardware failures	Moderate	Low	Training class on installed hardware and software	S		
(O)		Application lifecycle-software not upgraded or updated as new releases become available.	Large	Low	When notified by vendors that upgrades or updates are available, IT staff will install changes and test before apply to any systems.	S	With the implementation of Greenway, Weblz, ERAVE and other new applications for the agency, each of them come standard with 3 environments, Production, Testing and Training. We now have an environment where things can be tested prior to moving to production and IT is working closely with the programs to identify upgrades and update earlier so testing time can be adequately allocated before any pending deadlines.	
(O)		Lack of Controls	Large	Low	Assign security responsibility to ensure that adequate security is provided for the mission critical IT systems.	S		
(O)		Inadequate training	Moderate	Low	Conduct security awareness and technical training annually to ensure that end users are aware of the rules of behavior and their responsibilities in protecting Dept. of Health's overall mission.	S		
(O)		System degradation	Large	Medium	Monitor network performance with automated software tools.	S	Conduct periodic review of security controls to ensure controls are effective. IT's response since 2013 Risk Assessment findings: IT has purchased new network monitoring tools KACE, EqualLogic to help monitor the network performane as well as help identify trends or patterns that allow IT to take a more proactive approach. On the weekend of 3/29, IT will also significantly upgrade the network switches for the agency to a new platform and level of technology and move ADH from a 1GB base to 10GB. While it won't eliminate system degradation altogether the greatly increased speed and performance will pay dividends for the agency.	
(O)		Not doing backups	Large	Low	Do daily backup Provide backup capability(e.g., procedures for regular data and system backups)	S		
(O)		Loss of power	Large	Low	UPS Supports Servers and network room until Generator kicks in.	S	Full backups or snapshots of the data is done at least daily with differentials every 15-60 minutes depending on the application requirements. These tasks have been automated to make sure they happen on a regular basis.	
(O)		Improper Climate Control	Large	Low	Control the humidity and temperature of the computing facility (e.g., operation of air conditioners, heat dispersal).	S		
(O)		Security breaches.	Large	Low	Review building security Limit access to Computer room, lock all closet doors containing secure wiring, hubs, and cables.	S		
(FR) (O)		Loss of information	Large	Low	Off site tape storage at DHS.	S	IT has completed a comprehensive review of all access to IT rooms, areas and facilities and have removed access to all areas except for essential personnel. The list of users with access no is approximately 25% of what it was a year ago due to the review and removal of unnecessary access.	
(O)		Fire damage	Large	Low	Provide training on the requirements and procedures for the use of fire extinguishers and halon fire suppression systems.	S		
(FR) (O)		Theft of software	Moderate	Low	Limit access to ITS area and desktop support Agency software is kept in a locked area with restricted access.	S	IT has completed a comprehensive review of all access to IT rooms, areas and facilities and have removed access to all areas except for essential personnel. The list of users with access no is approximately 25% of what it was a year ago due to the review and removal of unnecessary access.	
(FR) (O)		Software viruses, spyware, hackers or security breach.	Large	Low	Install anti-virus on network and monitor firewall logs. Anti-virus programs runs automatically each time PC is turned on. Anti-virus program automatically updates itself from vendor website daily. Any unidentifiable email or incoming data is quarantined: firewall log will expose hackers.	S		
(O)		Newly installed software conflicts with other software.	Moderate	Low	All computers are pre-configured, before assigned to users. Users do not have administrator's rights and cannot install any software.	S		
(O)	Inadequate hard drive storage space for data.	Moderate	Low	Monitor space and provide backup for PC data.	S			
				Hard drive file space remaining is monitored constantly.	S			

(F) (FR) (C) (O)	Timekeeping	Missed Leave Time	Small	Low	1. Supervisor approves leave	S
					2. Timekeeper enters time in AASIS/Sends email to all IT of leave everyday	S
					3. Time checked/approved in AASIS	S
(F) (O)	Financial	Cut in Funds for IT salaries	Large	Low	Look for other funding from Programs to cover salaries	S
(F) (O)		Cut in Funds for IT Maintenance	Large	Low	Look for other funding from Programs to cover maintenance	S
(F) (O)		Overspending budget	Large	Low	Monthly reports from ADH FITS system show budget and expenditures.	S
(F) (FR) (C) (O)	Human Resources	Hire Unskilled IT Employees	Large	Low	1. Ask technical questions in interview	S
					2. Two IT personnel in interview	S
					3. Review/Approval for hiring	S

Management's Conclusion:

(x) The control activities are sufficient to mitigate all of the identified risks and provide a reasonable basis for achieving the stated objective(s).

() The control activities are sufficient to mitigate all of the identified risks and provide a reasonable basis for achieving the stated objective(s), except for the control activities listed as **not** sufficient in the Mgmt. Conclusion column. The new or additional control activities needed to mitigate the identified risk to an acceptable level are included in the Corrective Action Plan column along with an implementation date. The corrective action will be sufficient to mitigate the risk when implemented.

() Some control activities are **not** sufficient to mitigate all of the identified risks and provide a reasonable basis for achieving the stated objective(s). Management has not identified any control activities that would be cost efficient to implement in order to mitigate the risk to an acceptable level; therefore, we accept the risk that the stated objective(s) may not be achieved.

INTRODUCTION

The Arkansas Department of Health (ADH) is a unified health department, with a main office in Little Rock and 120 local health units in each of the State's 75 counties. Additional health units are located at local hospitals and remote areas.

ADH provides administrative assistance to these remote clinics through finance, human resources, information technology, legal, minority health, community support, health communication and marketing, tobacco prevention and cessation, policies and procedures, and facilities support. The mission of the Department is to protect and improve the health and well-being of all Arkansans.

Several key business initiatives are causing ADH to re-evaluate their current security management program. These include:

1. Future implementation of a United States Department of Agriculture (USDA) Electronic Benefit Transfer (EBT) system.
2. Compliance with State, Federal, and regulatory security requirements.
3. Enhancing security to address evolving security threats and leverage newer technologies.

ADH's primary compliance requirements include adherence to the USDA security guidelines, the Health Insurance Portability and Accountability Act (HIPAA) and other miscellaneous legislative requirements. ADH engaged IBM to determine if gaps exist in their compliance with the USDA EBT systems requirements prior to a planned EBT system implementation.

The recommendations in this report were derived from an analysis conducted against the Food and Nutrition Service's (FNS) [Electronic Benefits Transfer System Security Guidelines Handbook](#) dated February 2004. The recommendations are based on information gained during interviews with key IT and business management and reviews of documentation relating to security controls applicable to a future EBT system. Key individuals interviewed from ADH are listed in Appendix A of this report.

All security controls from the *FNS-EBT Checklist for Assessing Security Controls* were assessed. The *Checklist for Assessing Security Controls* may be found in Appendix A1 of the [Electronic Benefits Transfer System Security Guidelines Handbook](#).

The results of this analysis, which are included in this report, provide security strategy principles that ADH can use to make management and technology decisions consistent with the organization's security and business objectives. This information can be used as a foundation for plans to remedy identified issues, and to address security gaps before beginning to support an EBT system for FNS.

SUMMARY OF FINDINGS

The measure for conformance to the *Electronic Benefits Transfer System Security Guidelines Handbook* is the *Checklist for Assessing Security Controls* in Appendix A1 of the handbook. The handbook organizes IT Security Controls into four sections: 1) Management Controls, 2) Operational Controls, 3) Technical Controls, and 4) EBT Specific Controls.

ADH does not presently manage an EBT system. Therefore, many of the requirements in the handbook, especially those found under EBT Specific Controls, do not apply to ADH at the time of this assessment. When ADH proceeds with managing or implementing an EBT system for Arkansas, management should direct the use these additional controls as non-functional system requirements as part of the new EBT system. These requirements would either serve as basis for an in-house managed system, or as third party contractual requirements for an external systems provider.

The scoring of this assessment is based on substantial compliance or non-compliance with each control within the handbook's checklist. The questions in the handbook are designed to assess overall system security for an EBT system. Therefore, any conclusions drawn from the results of this analysis should consider the handbook's focus on system and operational security for support of an EBT system.

This analysis was conducted against the USDA handbook for EBT systems; however, most of the recommendations in this report will enhance ADH's security overall and are required by other regulations or initiatives, such as HIPAA and patient record exchanges.

Given the size of ADH staff, funding, training provided, and services provided, ADH has done remarkably well in addressing security on all fronts; however, ADH does have serious security gaps between their security practices and EBT standards. The procedural and technical controls required for EBT and not presently addressed by ADH are documented in this report.

It is not uncommon to find this number of gaps when evaluating against a new security standard, especially in an organization that has not undergone a health check or comprehensive audit. However, ADH should consider all the recommendations in this report as best practice, and are advisable to implement, whether or not ADH chooses to move forward with an EBT system.

The chart shown in **Figure 1** below depicts the overall assessment results in each of the four handbook categories.

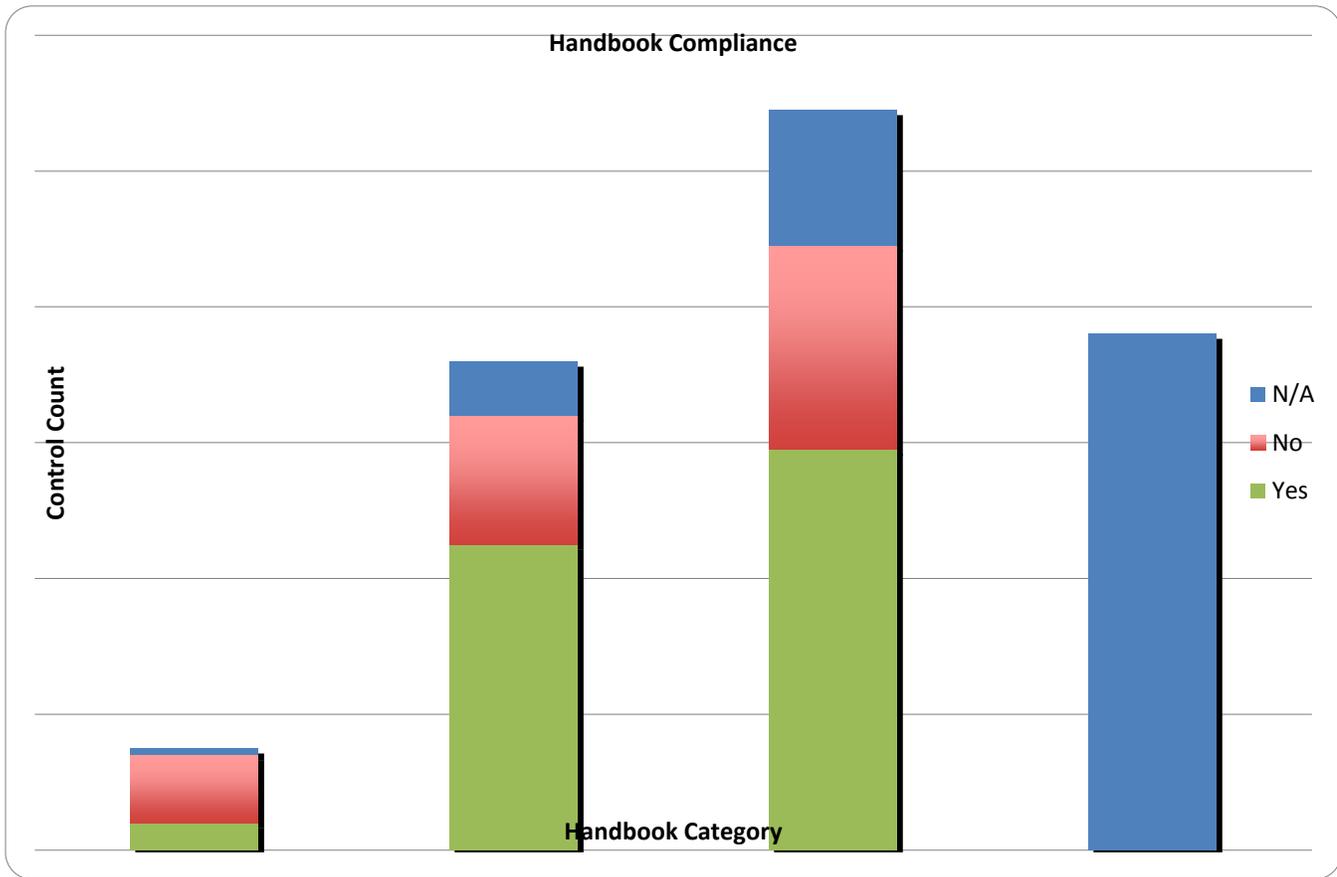


Figure 1

Although gaps exist between ADH security practices and the USDA handbook for EBT systems, three root causes contribute many of the findings. First, ADH does not presently have sufficient funding to implement enhancements and security systems typically used when managing sensitive personal information or electronic transactions. ADH also does not have the additional staff to support acquisition of additional infrastructure. Second, although security awareness is very important to the staff, ADH does not have written processes or established training programs to foster continued enhancement of sufficient security skills in key areas. Third, ADH does not have a security strategy that helps define what projects can or should be accomplished with the resources that are available.

Remediation Plan

Planning is a key component to strengthening an organization's security program. The recommendations in this report are important to the security of ADH systems and data, but not all recommendations can or should be addressed simultaneously. IBM has consolidated the recommendations contained within the report in **Table 1** below. Short term recommendations are activities that are immediately actionable and provide the most value for resources spent. Long term recommendations are important, but require significant funding and/or time to implement.

Short Term Remediation

2.1.1 EBT Security Program and System Specific Policy	
	Develop a 3-5 year security strategy plan.
	Develop formal documented security policies and procedures.
2.1.2 EBT Security Management Roles and Responsibilities	
	Security personnel should attend relevant security training.
	ISSO should be involved with any business process change to oversee security implementation.
2.2 OPERATIONAL CONTROLS	
2.2.1 Media Protection	
	A clean desk policy should be implemented.
	Employees should be required to log off and shut down workstations at night.
	Laptop computers should have power-on and hard disk passwords enabled.
2.2.2 Personnel Security	
	A separation of duties matrix should be developed and followed for security tasks.
2.2.3 Physical Security	
	The same process should be followed for immediately removing access rights (for voluntary or involuntary separation).
	A visitor log should be maintained for data center access.
	Adequate fire suppression needs to be provided in the data center.
2.2.5 Incident Response	
	ALL incidents affecting security need to be reported through management and documented.
	A security incident response contact list should be created and maintained.
2.2.6 Configuration Management	
	Patching should be implemented on a regular schedule within 30 days for high severity patches, and 60 days for medium severity patches.
	ADH should proactively monitor and manage critical patches for all systems and applications.
	Health checks should be performed to verify patches have been installed properly.
2.2.7 Security Awareness, Training & Education	
	Update initial and annual revalidation for security awareness, based on the findings of this assessment.
2.3 TECHNICAL CONTROLS	
2.3.1 Identification and Authentication	
	Strict password controls should be applied to all systems, devices and applications.
	Shared IDs should not be used.
	Privileged IDs that must be shared, should be escrowed and managed to provide auditability.
2.3.2 Logical Access Control	
	All default IDs should be disabled. Default passwords should be reset.
	Implement banners on all systems and applications to identify access to sensitive data and systems.
	Users should be required to log off at night and workstations rebooted for patches to be applied.
2.3.3 Auditing	
	Audit findings should be processed using the standard ADH tracking and incident handling procedure.
2.3.4 Internet/Web Security	
	Remote access should always be encrypted for administrative and development access.
2.3.5 Network Security	

	All network devices and firewalls should be patched following the ADH Patch Management Policy.
	Access to all network devices should only be allowed over encrypted connections.
	An appropriate level of logging should be configured for all network and firewall devices.
	Network logging should be maintained for a period of time in compliance with the established security policy.
2.3.7 Virus Protection Controls	
	Anti-Virus software should be implemented on all server systems (including UNIX systems).
	More strict web filtering should be implemented and monitored for compliance.
Long term remediation	
2.1 Management Controls	
2.1.2 EBT Security Management Roles and Responsibilities	
	3rd party contracts should require security policy compliance
2.1.3 Risk Management	
	A formal qualitative risk assessment should be performed.
	Regular internal and external vulnerability scans should be conducted.
	Penetration testing should be performed by a 3rd party.
2.2 OPERATIONAL CONTROLS	
2.2.1 Media Protection	
	Full disk encryption of all computers hard drives should be implemented.
	Encryption of all sensitive data on the network should be implemented (at rest, processing and during transmission).
2.2.3 Physical Security	
	All phone and network circuits should be fully labeled.
2.2.4 Contingency Planning	
	Formal business continuity plans should be initiated immediately.
	A BP plan needs to include provisions for the WIC application.
2.2.5 Incident Response	
	Formal incident response processes and procedures need to be documented and followed.
2.2.6 Configuration Management	
	Formal and documented Patch Management policies and procedures need to be created and implemented.
	Vulnerability management and testing should be implemented.
2.3 TECHNICAL CONTROLS	
2.3.2 Logical Access Control	
	User rights should be audited and reviewed regularly for validation of access requirements.
	All ACL rights should be regularly reviewed for compliance to policy.
2.3.3 Auditing	
	Auditing and reporting on all system logs should be conducted regularly and in an automated process if possible.
	Audit policies need to be developed, documented and applied.
	A central logging and reporting facility should be implemented.
	Log and report review should be conducted by independent personnel.
2.3.4 Internet/Web Security	
	Security should be integrated into all development SILK projects.
	The development staff needs to be trained in implementing security into the SDLC.
	The network should be segmented into tiers for security access control and isolation.

	Firewalls (or packet filtering) should be implemented at perimeters around all network tiered zones.
	Web and application servers should be located on separate network segments from end point connections to them.
	Trust relationships between systems should be removed (or heavily restricted) between security zones.
	The development team should not use real (sensitive) data in development and testing environments.
	Documented policies should be created and followed for implementing software controls throughout the ADH infrastructure.
2.3.5 Network Security	
	IDS systems (HIDS and NIDS) should be implemented throughout the network.
	Monitoring of network activity should be performed.
	A network vulnerability assessment should be implemented.
2.3.6 Database Security	
	Sensitive data in all databases should be encrypted.
2.3.8 Penetration Testing	
	Penetration testing should be performed at least annually.

Table 1

USDA IT SECURITY GUIDELINES

FNS-EBTS HANDBOOK

According to 7 Code of Federal Regulation Seven (7 CFR), Sections 277.18 (P)(2), ADP Security Program, "State agencies shall implement and maintain a comprehensive ADP Security Program for ADP systems and installations involved in the administration of the Food Stamp Program." FNS developed this guideline to assist states in developing security programs that protect EBT Systems.

The USDA guidelines are detailed in the handbook and this is the primary compliance model the GBS team used to perform the security assessment against for the ADH.

The USDA FNS-EBTS IT security requirements are organized into 4 domains. The four domains are as follows:

1. Management Controls
2. Operational Controls
3. Technical Controls
4. EBT Specific Controls

The following sections discuss the 4 categories of the FNS-EBTS IT security standards along with relevant high level findings for each of the categories.

2.1 MANAGEMENT CONTROLS

2.1.1 EBT Security Program and System Specific Policy

USDA Controls

Program security policies are broad and establish the security program and enforce security at the program management level. System-specific security policies are detailed and enforce security at the system level.

All organizations that process, store or transmit EBT information must develop, implement and maintain an IT Security Program to ensure the protection of EBT information. The IT Security Program must include appropriate protection for the EBT resources within their organization to include hardware, software, physical, and environmental facilities.

The EBT program security policy establishes the security program, assigns the appropriate security personnel and outlines the security duties and responsibilities for all individuals within the program.

The EBT program security policy will encompass all the appropriate security controls contained in this guidelines handbook under *Management Controls*, *Operational Controls*, *Technical Controls* and *EBT Specific Controls*. Security controls shall be cost effective and based on a risk assessment, as outlined in Section 2.1.3, *Risk Management*.

System-specific security policies for EBT systems will be enforced through logical access controls as well other technical security configuration controls.

Findings

ADH has very few documented standards and processes relative to information security and does not have a formal security plan that is updated annually. An EBT System has not been established for the State of Arkansas. A feasibility study is being conducted for EBT, and implementation is expected in 2012.

Although ADH does not have a formal Security plan in place, they have outlined many security projects to initiate when funding and resources become available. An information security policy is currently under development.

Risk and Impact

A security strategy outlines an organizational security plan that addresses an organization's security needs for long-term business initiatives. The absence of a plan typically allows business initiatives to proceed with little or no security when the security controls took more time or resources than originally anticipated.

A security policy determines corporate directives with regard to information security goals and objectives. It provides security guidance to management, end users, application developers and

others by defining the security parameters within which all must operate. Poorly defined or ambiguous rules or policies can put the organization and its information assets at risk unnecessarily. These risks can result in financial loss, litigation, or loss of its customer base. On an individual level, the lack of a well defined security policy and supporting security program may result in the organization's inability to identify and take disciplinary action against an individual or group of individuals who violate security policies or commit a crime. A security policy, along with the associated standards and procedures, also provides the foundation for a mandatory and regular review cycle. This review cycle is required in order to maintain adequate response to incidents, changing technologies, and business model changes.

Recommendations

Use organizational initiatives, audit findings, existing security project plans, and this report to create a three to five year security strategy for ADH. Develop formal, documented policies and procedures for security and implement a process for regular auditing with external and internal reviewers and updates as necessary.

Action: Create group to formalize plan.

2.1.2 EBT Security Management Roles and Responsibilities

USDA Controls

This section will not be able to capture the uniqueness of all organizations, but will provide a basic template and outline the responsibilities that should be performed under each role:

1. **Senior Management.** Provides the high-level direction for carrying out the organization's mission. They are ultimately responsible for the overall security of the organization, including the security of IT systems and the assurance of mission-critical operations.
2. **Information System Security Officer (ISSO).** The ISSO is appointed to develop, administer, and maintain an adequate information system security program. The ISSO directs the organization's day-to-day management of its computer security program. This individual is also responsible for coordinating all security-related interactions among the organizational elements involved in the computer security program as well as those external to the organization.
3. **Technology Providers.** Assist the ISSO in implementing and administering system-specific security controls. Systems and/or network administrators under the oversight of the ISSO securely configure EBT systems such as:
 - a. System/Network Administrators.
 - b. Help Desk.

Findings

ADH has no formally trained ISSO or defined information security organization that can coordinate security functions, implementations, and compliance across the entire organization. This is primarily a function of ADH's size present level of funding. ADH has not documented duties or responsibilities for those acting in security roles. Staff responsible for security activities, also perform administrative and compliance related tasks resulting in a lack of separation of duties. No formal education or training has been provided for those who perform security tasks other than occasional conference participation. Critical security responsibilities are not formally defined by policy and changed as business conditions vary.

Risk and Impact

A dedicated security officer acts as a central authority for security-related issues, and a single point of contact for security incidents. A security officer provides a counterpoint to operational activities in providing a separation of duties.

Employees have little in the way of access to trained security resources or focal points to call whenever a decision must be made concerning security controls on the information assets they own. This deficiency results in less efficient management of security issues

The responsibility of defining security standards for service providers lies with the parent organization. Technology providers that do not have security standards from which to operate may use their own standards that do not address the parent organization's regulatory requirements. Contracts with

service providers that do not require adherence to the parent organization's security standards results in the service provider using their own, perhaps weaker standard, or none at all.

Recommendations

ADH security personnel should attend relevant security training for establishing security standards, managing security systems, responding to incidents, developing secure applications, and security within the systems lifecycle.

ADH should establish third party information security standards, initiate or renegotiate contracts with partners that require adherence to these standards, and establish an oversight process to monitor compliance of third parties against these standards. The ISSO (or appropriately trained representative) should be actively involved when new or changed business processes are developed to make sure any necessary security requirements and compliance are integrated in the initial stages of development.

Action

Created 5 year IT plan. ITS committee peers have a project to rework the Policies and Procurers.

2.1.3 Risk Management

USDA Controls

Risk management, when applied to EBT systems is a continuous process of identifying threats, determining risks, determining security controls and selecting the most cost effective controls.

EBT business areas and "owners" of information systems should conduct a risk assessment for each system. Since a major change to the system could adversely affect the protection profile from the last risk assessment performed, a new risk assessment should be performed whenever there is a major change to the information system.

Findings

ADH has not conducted a formal risk assessment or penetration test.

Vulnerability scanning has been performed in the past, but not on a regular basis. Sensitive assessments would be stored in the acting ISSO's office or on a protected network share.

Risk and Impact

Risk assessments help an organization determine how best to allocate resources to security assets. Critical assets, those at the greatest risk of being exposed, then receive the most attention as directed by the organization's security strategy. A formal risk assessment identifies information assets, the systems they reside on, and the environments they reside in.

Each asset is examined for potential threats, the frequency of the threat, and the impact of each threat to the asset. The resulting risk is a function of the frequency and impact of each threat.

Risk assessments are also occasionally defined as vulnerability scans or penetration tests. Although vulnerability scans and penetration tests can identify the most commonly understood threats to information systems, other threats exist such as natural disasters, service availability, and insider malfeasance.

Recommendations

ADH should conduct their own qualitative risk assessment using a list of all ADH systems and assets as a starting point. This risk assessment can be used to prioritize security spending within a security strategy or security plan. A formal risk assessment can be conducted when funds permit.

Regular internal and external vulnerability scanning should be conducted using an in-house system or by contracting with a third party provider as a managed service. Penetration testing should be conducted by a third party provider when funding is available.

Action

Implemented a plan to find owner' for IT systems. This is to include "Champions" for all ITS system/applications with a list of all systems. Penetration testing list in later section 2.3.8. ISSO to join state committees on Security Management in order to be aware of State planes. ISSO to attend Security Training. ISSO to join Infer Gard.

2.2 OPERATIONAL CONTROLS

2.2.1 Media Protection

USDA Controls

Media controls need to address the storage, retrieval, and disposal of sensitive materials that should be protected from unauthorized disclosure, modification, or destruction. There are two forms of media control to consider:

1. **Computer Output Controls:** All printout copies of sensitive EBT information should be clearly marked as such. If required, sensitivity levels with the associated labels may be required to identify different sensitivity levels of EBT information. In addition, procedures for storage, mailing, marking, and disposal for the different levels of sensitive EBT information may also need to be defined.
2. **Electronic Media Controls:** All the requirements (labeling, storage, mailing, etc.) for computer outputs should be applied to electronic media that contain sensitive EBT information. Procedures need to be established to ensure that data cannot be recovered from electronic media that contains EBT information before transfer, reuse (non-EBT related) or disposal.

Findings

ADH does not have a cryptographic strategy in place and relies on business partners or auditors determining when additional protection needs to be applied to information assets. ADH does provide encrypted USB drives for portable storage and uses encryption on VPN links. There is a project currently being deployed to provide PGP disk level encryption to all computers and removable memory sticks, but has not been fully implemented at the time of this assessment.

ADH does not utilize encryption on servers, databases, applications, or during transmission across the internal network. Encryption is not used for sensitive data, financial data, off-site backups, remote administration, desktops, or hard drives in unsecured locations.

Reports are rarely printed, but locked storage is not available for use when they are printed, and ADH does not have a clean desk policy to validate controls for secured access to sensitive data throughout the organization.

Tapes are labeled but do not indicate if data is sensitive or not sensitive.

Risk and Impact

Without clean desk policies and data classification, documents and data can be accidentally made available to unauthorized personnel. A clean desk policy not only falls into the category of physical security, but also into security standards. In addition, since many sites are remote, physical security is less restrictive internally and can propagate additional exposure or leakage of sensitive data.

If small offices are not secured, all removable media are allowed, and the internal network architecture is not broken down into several security zones, data can still easily be leaked and malware introduced from unsecured physical locations.

Without a consistent organization-wide encryption policy, variations in the way data is protected could expose otherwise protected data. The unauthorized disclosure or modification of this type of data could put ADH in legal or regulatory jeopardy.

Identifying systems, applications, and media that contain sensitive data is necessary to assess the risk and subsequent controls required for protecting the data. However, security experts are divided on whether media should be physically labeled as sensitive or not. Physical labeling data as sensitive reminds contentious employees to protect it, but also identifies the data as a high value target.

Recommendations

Adherence to a “clean desk” policy should be required, stating that all employees log off (or lock the computer screen of) their computers when leaving their desk for any reason and to log out and power down when they leave work for the day. Any sensitive or critical data or equipment should be securely stored when left unattended in an unsecured area. Additionally, ADH should mandate that users of laptop computers use power-on, or disk encryption passwords to assist in protecting valuable ADH information assets.

ADH should proceed and finish deployment of the full disk encryption project for all computers, and provide a method to validate compliance and provide remediation steps for violations.

Regulation and best practices also calls for encryption of sensitive personal information, financial data, and medical records. ADH should initiate an encryption strategy to cover databases, applications, transmission encryption between the desktop and web server, the web server and application server, and application server and database. The encryption strategy should extend to backups. An initial step could be the implementation of web server SSL level encryption for ALL web portal access when sensitive data is accessed, and the use of native database table-level encryption within SQL servers for sensitive data. The implementation and mandatory requirement for non-encrypted remote access to systems should also be developed.

Action

Create Group Policies to manage the desk tops and servers. Using inactive timers for PC's to lock the PC. Using End point encryption an all mobile PC(Laptops). Change the user LOGON to using WEB base application experience of RDC to manage by a role base model. All Tapes are treated data sensitive.

2.2.2 Personnel Security

USDA Controls

All personnel with responsibilities for the management, operation, maintenance, or use of EBT system resources and access to sensitive EBT information should have the appropriate management approval. An employee's access to EBT systems should be restricted to the required resources that the employee needs to fulfill his or her duties.

The following personnel security controls should be enforced on all EBT systems:

1. The ISSO or the system owners who directly support business operations should authorize, in writing, any non-EBT personnel who use their system.
2. Technical support personnel from outside EBT, who perform maintenance on EBT systems within EBT-controlled facilities, should be escorted at all times, unless they have been approved for unescorted access.
3. All employees must be removed from the system on or before their employment termination date.
4. An employee's access to the system should be removed prior to notifying the employee of termination procedures.

Contractor Personnel Requirements: All contractors accessing EBT systems should sign a non-disclosure form as a condition of receiving EBT accounts. The ISSO shall provide non-disclosure forms and maintain completed forms. Contractors should be required to follow the same personnel security requirements as State employees.

Separation of Duties: Separation of duties ensures that no single individual has total control of the system's security mechanisms; and, therefore, no one individual can compromise the EBT system completely.

Findings

ADH institutes solid practices for managing personnel security, and manages security consistently against these practices. Primarily due to the size of the IT staff, ADH does not have employees dedicated to information security.

Risk and Impact

Existing operational personnel conduct all security tasks. This practice results in an operational environment that does not have a clear separation of duties, and lacks proper governance. A lack of overall security organization represents high risk to the company in the on-going maintenance of a security policy and in the protection and validity of its information assets.

Recommendations

ADH will likely not be able to appoint a dedicated ISSO. In the absence of an ISSO, a separation of duties matrix should be developed so that operational security tasks are not performed by production support resources, and to ensure that more than one individual is required to perform key tasks. Critical security tasks include functions in setting policy, system hardening, incident response, identity management, security architecture, and application development.

Action

We have implemented all parts of this section.

2.2.3 Physical Security

USDA Controls

All hardware, software, telecommunications, documentation, and sensitive information handled by a system should be adequately protected to prevent unauthorized access, use, modification, disclosure, or destruction.

Physical security policies and requirements for EBT computer facilities must include physical construction, fire protection, access controls and environmental controls.

Rooms containing system hardware and software, such as local area network rooms or telephone closets, are secured, where possible, to ensure that they are accessible to authorized personnel only.

Servers and mid-tier systems not housed in a central facility must be afforded protection from unauthorized access and both intentional and accidental damage. The following physical security procedures shall apply:

1. Access to these systems shall be physically controlled
2. The rooms or cabinets that house this equipment should be secured
3. Environmental controls (separate air conditioning, fire protection, etc.) may be warranted.

The physical security protection employed in the centralized computer facility should be commensurate with the maximum sensitivity of the EBT information handled. Computer rooms processing EBT information and those approved for open storage of EBT information should provide a separate level of access control (separate from main building) for protection of the restricted area. Unescorted access to administration areas is limited to personnel who have official business in the area or have approval of the ISSO. The following physical security procedures should apply:

1. Establish internal access control procedures (zoning)
2. Use identification badges for physical recognition
3. Require contractor or vendor badges to be clearly identified as such
4. An intrusion detection system (alarm) should be used to monitor the perimeter and interior of the computer room
5. Use a closed circuit television (CCTV) to monitor access to the computer room and its critical assets.

Findings

Employee access is not removed immediately for voluntary employee separation, although it is removed immediately for involuntary separation. A visitor's log is maintained for access to ADH's main facility, but a visitor's access log is not maintained for access to the data center. Most, but not all phone and network circuit are labeled. Fire suppression is not available for part of the data center.

Risk and Impact

Removal of system and physical access for involuntary separation is critical. Removing system access for employees who separate voluntarily is usually not a serious security concern, but an issue

that is a frequent compliance failing. The biggest risk exists when access is not removed after several days.

A visitor access log recorded in the data center helps with incident response, forensics, and audits in determining which visitor had access to critical system resources at a given point in time.

Recommendations

Use the same procedure for removing system and building access immediately for employees who voluntarily separate from ADH for all employees.

A written log should be maintained within the data center for all visitor access.

Fully document and label all phone and network circuits, and provide adequate fire suppression in the data center (per State requirements).

Action

We have implemented all parts of this section.

2.2.4 Contingency Planning

USDA Controls

Each major EBT application and general support system must have a viable and logical Contingency Plan. This Plan will be routinely reviewed, tested, and updated to:

1. Minimize damage and disruption caused by undesirable events;
2. Provide for continued performance of essential system and computer processing operations, services, and mission-critical function.
3. The ISSO and appropriate systems personnel (system owner) should coordinate to develop and maintain a current, viable Contingency Plan.

Contingency Plans include the following:

1. Backup operations plans, procedures and responsibilities to ensure that essential (mission-critical) EBT operations will continue if normal activities are stopped for a period of time.
2. Emergency response procedures that include civil disorder; fire; flood; natural disaster; bomb threat; or other incidents or activities where lives, property or the capability to perform essential functions are threatened or seriously impacted.
3. The lowest acceptable level of essential system or functional operations, so that plan priorities may be made. This must include provisions for storage, maintenance and retrieval of essential backup and operational support data.
4. Post-incident recovery procedures and responsibilities to facilitate the rapid restoration of normal operations at a primary site or, if necessary, at an alternate facility, following destruction, major damage or other significant interruptions of the primary site.

Contingency plans should be tested periodically (biannually) to ensure accuracy and completeness.

Findings

ADH has not created a business continuity plan (BCP) and is presently working on a disaster recovery (DR) plan. ADH has planned for reaction to some incidents, such as bioterrorism, but has not yet factored natural disasters or catastrophic system events into these plans. ADH follows State DR practices, and has integrated contingency planning with DR when applicable.

ADH does have the ability to recover some operations in the event of a disaster. The State's Department of Information Systems (DIS) houses ADH'S DR systems. DR tabletop exercises have been performed, but this capability has never been physically tested. Network routing plans have been discussed but not implemented. Most fiber networks are not redundant.

ADH determined that local health units can operate independently for up to 1 week before the data collected needs to be processed. Women Infants and Children (WIC) is the only application that must have continuous availability.

Backups occur multiple times daily for some systems, and nightly for others. Both incremental and full backups are performed, although some systems (such as Exchange email) do not perform any full backups. Backup tapes are not locked securely within the data center, but a cabinet is available for that purpose. Tapes stored in the data center are available to any IT staff with access to the area.

Risk and Impact

Incident response, disaster recovery, and business continuity only work properly when planned in advance and the event has been anticipated. Without recovery plans, organizations will, at a minimum, take an extended period of time to recover. Without redundancy, recovery may not be possible.

Should an event occur that results in the loss of individual or institutional knowledge of employees or service providers, ADH would have difficulty resuming operations. Without documented processes and procedures to resume operations, ADH would incur considerable expense.

Recommendations

A preliminary Business Continuity Plan and Business Impact Assessment should be created. The following decisions should be considered and integrated into the Business Continuity Plan:

1. Level of disaster recovery (DR) to implement (for example, warm-site vs. cold-site, etc.)
2. Business continuity and DR procedures for all business and technology units
3. How ADH can leverage State plans and infrastructure
4. Roles and responsibility assignments for key managers and staff
5. Periodic testing of business continuity plans

ADH does have the luxury of distributed operations (health clinics) being able to continue in their primary function without system availability. However, just one application needing DR capability (in this case, WIC), requires a DR plan and services.

Action

Backups are completed on all system daily and are located at different and secure location. Business Continuity plans are always part of our discussions. The DR planning is in a stage where we are redefining how and what DR means. There is a project Group working on this issue.

2.2.5 Incident Response

USDA Controls

A security incident is any event or condition that has the potential to impact the security of an EBT system. Examples of reportable incidents are:

1. Discovered viral infection
2. Discovered malicious code (i.e., viruses, trap doors, logic bombs, worms, Trojan Horses, etc.)
3. Uncovered hacker activity
4. Discovered system vulnerabilities
5. Unauthorized attempt, successful or not, to access an EBT system
6. Deviation from security policy
7. Other unusual activities

If malicious code is detected, whether prior to system entry or after system infection, or you detect a security violation that may result in:

1. Disclosure of sensitive information to unauthorized individuals,
2. Unauthorized modification or destruction of system data, or loss of computer system processing capability, or
3. Loss or theft of computer system resources (report it to your supervisor or other appropriate supervisory channels, as a security incident).

The incident must be promptly reported to the immediate supervisor. The supervisor will in turn report the incident to the ISSO for technical resolution. The ISSO documents and reports the incident, as appropriate, and address the impact of the security incidents.

When reporting an incident, the following information must be provided:

1. Type of incident.
2. Date and time of the incident.
3. Name of the victimized system.
4. Description of the incident.
5. Impact of the incident.

Findings

ADH uses an undocumented process to handle incident management. ADH does not have written policies that address the detection, reporting, and responding to information security incidents. All employees are trained how to report any security incident during user orientation.

The ISSO responds to all IT related security incidents and is responsible for resolution. No classification is performed for different types of incidents. Root cause analyses are not formally performed or documented, but incidents are discussed each week.

Procedures exist for regional health-related incidents, but not for the collection, retention, and presentation of evidence for virus outbreaks, theft of equipment, data breach, or employee theft.

Risk and Impact

In the absence of a formal, documented incident response policy and processes to support that policy, ADH is at unnecessary risk from major security incidents due to inconsistent response, delays, and regulatory requirement non-compliance.

ADH is exposed by the inability to respond appropriately to security incidents in a timely manner due to the lack of properly documented and widely distributed information security incident response process and lack of training in its implementation. This puts business functions at risk of being curtailed or stopped for a longer period of time than would be the case if a properly documented response process were in place.

Recommendations

A formal incident response process and procedure needs to be established and documented.

All incidents affecting security should be reported through management channels as quickly as possible (including virus incidents). Procedures should include root cause analysis, integration of findings into security standards and operational procedures, and detail how collection of evidence should be managed.

A contact list for incident response should be created and maintained that contain names, job titles, phone numbers and e-mail addresses for subject matter experts, operations management, security contacts, and appropriate civil authorities.

Action

The ISSO has been to training on procedures on formal incident response. The process is in a policy statement .

2.2.6 Configuration Management

USDA Controls

Configuration management:

To be effective, configuration management must be applied to the full life cycle of activity involved in building and implementing business applications and the EBT infrastructure. The discipline consists of a set of processes that produce and validate components such as the configuration items (CIs) for the EBT systems environment. All components that are to become part of the EBT systems environment (including EBT inventory information) need to be deposited and maintained within a configuration management database (CMDB) where the information can be referenced by other management functions.

The first steps in developing the configuration management plan (CMP) are to define the scope and objectives of the configuration management process and to identify specific business goals to be achieved. Both short and long-term objectives should be defined.

Configuration management applies to all EBT infrastructure systems and equipment. To ensure the usefulness of the configuration management process, EBT organizations should:

1. Identify and label all CIs in the EBT environment
2. Control and track all changes to CIs throughout the system life cycle
3. Coordinate the documentation of all changes to the EBT environment with change management
4. Establish and maintain baseline configurations
5. Control assets by knowing what assets are held by the organization
6. Manage software licenses and ensure that only authorized copies of software are used in the EBT environment
7. Conduct audits to ensure that the actual state of the EBT environment matches what is documented in the CMDB
8. Train organizational groups about the CMP process and the importance of using only authorized CIs in the EBT environment
9. Provide reports to management.

Change management:

Change management is responsible for changes in technology, systems, applications, hardware, tools, documentation, processes, and roles and responsibilities. The security goal for change management is to identify all proposed changes to affected systems and processes before the change is implemented in order to mitigate or eliminate any adverse effects on the security posture of the system.

Change management should manage changes that:

1. Will affect multiple users/customers

2. Could potentially disrupt mission-critical functionality
3. Involve hardware (such as servers) or software modifications
4. Involve operational and process modifications that affect multiple users/customers.

Findings

ADH does not use configuration management processes within their systems environments. ADH does have separate development, test, and production servers, but they reside on the same network.

Change management processes have not been developed, but ADH has the practice of patching high risk system vulnerabilities on Windows systems. Other platforms and applications are not patched for security purposes.

Application development personnel have limited access to make changes to production servers, although within test and development environments they have much greater access.

Risk and Impact

Separation of development, test, and production networks helps IT discover software issues before a system is placed into production. Isolating these systems on separate networks is essential to keep vulnerabilities in development and test systems from affecting related and non-related production systems.

System patches are the easiest way to secure the most exploitable security weaknesses. Some network operating systems, such as Windows, make patching very easy. Other systems, such as database servers and network devices, are more difficult but may place ADH at even more risk if not patched.

Without proper system patching policy and procedure to guide administrators, there will be fatal security flaws within the infrastructure. This specifically pertains to security patches that fix critical vulnerabilities. Whether from mis-configuration, internal errors, or conflicts in software, patching is a necessary process for business continuity.

Recommendations

It is recommended that ADH create a set of documented policies and procedures for system patch and change management. Once created and approved by IT security, the various system groups can implement the plans and continue this process on an ongoing basis for patch and change management.

The security team or system administration should proactively monitor vendor web sites and security research web sites for both security patches and security vulnerabilities. The risk these vulnerabilities pose to ADH should be categorized and deployed based on a fixed schedule, set by policy. Remediation should be tracked and any deviation to the schedule should be escalated. Regular and periodic audits should test for the remediation of these vulnerabilities.

System patches identified as High risk should be implemented within 30 days, and Medium risk patches within 60 days. Low risk patches should be implemented as soon as possible after more

critical patches are applied, if their requirement is deemed necessary during a formal review. Patches should be applied to all operating systems, network devices and applications and documented in the ADH ticketing or a tracking system for audit and review. Patching should occur on a defined schedule for all operating systems, network devices, security systems, applications, and middleware.

ADH should define and implement a coordinated process to address the discovery, identification, remediation, and prevention of vulnerabilities. This can be attained with the implementation of a well-defined vulnerability management plan as indicated by industry best practices and security standards.

Development, test, and production environments do reside on different servers, but these servers should be isolated on separate networks. Application development personnel access to each environment should be regularly reviewed and adjusted as necessary. Strong limitations should be in place especially for production systems to help maintain system integrity controls.

Action

We have moved 80% of our server to VM Ware server Farm. This has made our Configuration management simpler to perform. The configurations are now part of our backup plan. Also the DR plan will have configuration management as part of the its plan. There is a project group working.

2.2.7 Security Awareness, Training & Education

USDA Controls

Personnel who manage, operate, program, maintain, or use the EBT System should be aware of their security responsibilities. Security awareness training should be provided in addition to functional training before system users are allowed access to the EBT System. This training should be conducted periodically (e.g., once a year).

ISSO's have a very important function within their organization and therefore, require a comprehensive and continuing security training program.

Security awareness training should be mandatory and should be completed prior to granting access to the system. Periodic refresher (annual) security training should be required for continued access. Therefore, each user (including contractors) must be versed in acceptable rules of behavior before being allowed access to the system. The training program should also inform the user on how to identify a security incident.

Initial User Briefing:

Training should be provided to all new users of a system. This training should include general security awareness issues, such as viruses and hackers, as well as an awareness of system specific security requirements. Users should also be allowed to review a copy of the EBT Security Policies document.

System Security Refresher Training:

Periodic, but at least annual, training should be provided to all system users. Training should include reminders and updates of computer security awareness and system specific security requirements. Periodic system security training will be documented and maintained on file.

Findings

ADH maintains a security awareness and training program, which is heavily weighted on HIPAA compliance. All users are required to complete training before accessing any computer system, and this training is mandatory to repeat annually.

ADH IT employees do not have formal information security training, but ADH employees interviewed exhibited an understanding and application of many basic security concepts.

Risk and Impact

A security awareness and training program is paramount to maintaining security, and perhaps the most critical aspect of maintaining information security at any level. Managers, employees, and system administrators must all understand their role in maintaining security within the organization.

Recommendations

ADH's initial user security orientation and system security revalidation training should be updated to address any corrective action taken as a result of findings from this assessment.

Action

We have implemented all parts of this section.

2.3 TECHNICAL CONTROLS

2.3.1 Identification and Authentication

USDA Controls

User Identification (User ID) is used to identify persons working on EBT systems. For this reason, all User IDs should be unique throughout the system. The GBS team has analyzed the statement “Passwords should also be unique within the system” to mean that an individual using multiple IDs should use unique passwords for each ID. The User ID and password for each individual identifies that individual to the system and must be protected to ensure that no one can impersonate that individual.

Passwords:

Use of passwords should be required within EBT systems. Password policies for EBT systems should consist of the following:

1. Minimum password length (eight (8) alphanumeric characters recommended)
2. Password history kept to prevent reuse of current passwords
3. Limit incorrect password attempts (three (3) unsuccessful attempts is recommended)
4. Procedures for password changes (every 60-90 days recommended)
5. Account lockout procedures established (after three invalid attempts)
6. Procedures for password changes
7. Procedures for handling lost or compromised passwords
8. Auditing for inactive accounts (30 days of inactivity).

The password policies should be communicated to all EBT system users during the initial security training and periodically during refresher training.

Findings

Some infrastructure systems use a shared ID known to a small set of support staff. Password policies are enforced on the Windows platform only. Auto-expiring accounts are not used.

Risk and Impact

Shared user IDs may be compromised and used for unauthorized activity without detection. Additionally, authorized individuals may cause unintended or deliberate harm to systems and access sensitive data without being detected since the use of the IDs are not assigned to any one individual and use of the IDs is not monitored.

Shared IDs are a risk because user actions cannot be audited and users cannot be held accountable for actions. Service disruptions can occur for other users if secondary users are not alerted to password changes.

Shared IDs are acceptable in some limited circumstances, but shared IDs should be a documented and tracked exception to an organization's security policy. Shared IDs should be severely restricted in their use, or eliminated completely when possible.

Recommendations

Password controls should apply to all operating systems, network devices and applications, in addition to the controls required for Windows.

Shared IDs should not be used. Training systems, temporary systems, or systems with very limited network or application access are exceptions that should be reviewed by the ISSO. Application access to databases using credentials should be documented and managed with unique IDs. Privileged credentials that must be shared can be secured by holding them in escrow, or by using techniques such as splitting the password across multiple users.

Action

We have implemented a new badging system controlled by ITS HelpDesk and our HR group. Our Policy and Procedures document are written and the employees read then verify that they have read the Policies.

2.3.2 Logical Access Control

USDA Controls

ADH implements a separation of duties and access control restrictions for all IT support and system management staff.

EBT supervisors and managers shall continuously assess the privileges granted to employees and contractors and submit the necessary requests to change or remove access to those system and network resources that are no longer required.

Access to the EBT systems should be controlled through the use of access control devices designed to restrict connections to the EBT network and its resources. Access control devices such as firewalls and routers should be deployed within the network infrastructure to restrict traffic into and out of the EBT network.

System Accounts:

To establish an EBT account, a supervisor or manager should request the account and password, in writing.

1. No more than one system account should be permitted unless the position or job function requires multiple accounts. For example, a system administrator should have two accounts: an administrator account used when performing system administration functions, and a user account for routine day-to-day use.
2. All guest accounts should be disabled on EBT systems.
3. All default system accounts should be disabled or removed.

Workstation Security:

All EBT workstations should require password-protected screensavers. Workstation screensavers should be configured to activate when the keyboard or mouse is not used for a configurable period of time (15 minutes recommended), requiring reentry of a password before access is granted.

Users should be required to log off their workstations every night to shutdown the system. Users should be instructed to lock or log off their workstations if they are going to leave it unattended for a significant period of time.

Warning Banner:

Warning banners should be displayed before any access to an EBT system is authorized. Where technically feasible, warning banners should be displayed upon logon to any EBT system. Warning banners are an important legal instrument and should be crafted to inform users that they are accessing a government system and are subject to legal penalties for unauthorized access or misuse.

Findings

Warning banners are only implemented for Windows system logins, but not when accessing sensitive data (such as through the Common Customer web application).

ADH suggests logging off or shutting down a machine when a user leaves the machine unattended, but it is not a requirement. There is a Windows Active Directory Group Policy enforcement for a password protected screen saver to activate after a period of inactivity on Windows computers only.

Default accounts, such as the Windows guest ID, are not disabled.

Risk and Impact

Without processes in place to periodically assess user access rights it is possible that access to sensitive materials have been granted as well as access rights to users who are no longer with ADH, demoted, and/or should not have access and ADH has no way to determine this. Such improper access right grants could lead to information leakage as well as possible misuse or destruction of data.

Just as user access controls change and become misappropriated, so do system-level access controls. Systems, applications, and architectures must be evaluated against changing organization standards through a routine process, or risk deviation from evolving organization standards and lack of thoroughness and diligence on the part of application developers and system operators.

Users not logging off computers at night is an issue for security because it is difficult to apply patches and updates when they cannot trigger a system to reboot. Any user inactivity timeout provides the greatest protection, but having users log out is preferred, especially when the device is mobile or located in remote areas.

Recommendations

All default IDs should be disabled, or have default passwords modified. Access logs recording use of these IDs should be the focus of any access control auditing process.

Perform regular audits of user access rights, which is different from scanning for inactive accounts.

Systems and applications should be regularly reviewed through a governance process to ensure system and application-level access controls are implemented according to ADH standards.

Banners should be implemented on ALL systems (including network devices and in application interfaces) to comply with stated security policy requirements, and should include wording to address access to sensitive data or systems as appropriate.

A method should be implemented to force end-user systems to logoff or reboot at night so that patch management is not interrupted. If this is not possible, patches should be applied when available and forced reboots should be implemented using the current Windows Update Services and Active Directory Group Policy controls.

Action

We have implemented all parts of this section.

2.3.3 Auditing

USDA Controls

Audit trails should capture the following information:

1. System start-up and shutdown
2. Successful and unsuccessful login attempts
3. User actions to access files or applications
4. Actions taken by system administrators and security personnel
5. All administrative actions performed on an EBT system.

Audit trails should record the following information for each event:

1. Date and time of event
2. Type of event
3. Success or failure of an event
4. Name of file or application accessed.

Audit Trail Maintenance:

Audit trail logs should be properly secured with access limited to system administrators and the ISSO. The ISSO should regularly review the audit logs. The following procedures should be required for maintaining audit trails:

1. Review of audit trails is a function of the ISSO or designee.
2. Audit trails should be reviewed weekly at a minimum, but preferably daily. Depending on the size of the system, the review can consist of the entire audit trail, a review of customized reports, or using an automated audit-monitoring tool.
3. Access must be controlled to prevent unauthorized access, modification, or loss.
4. Audit trails should be maintained for one (1) year in either paper or electronic form.
5. Paper copies of audit trails should be treated as FOR OFFICIAL USE ONLY and shredded when no longer needed. Electronic copies must be cleared in some manner before disposal. (See Section 2.2.1 Media Protection.).

Findings

ADH uses Microsoft's standard recommendations for logging of system and security information, but does not actively monitor any security events. No logging of any other extended information or access information is performed on Windows systems. ADH logs extensive information on firewalls and the Common Customer Application, but not as much on other infrastructure systems and applications. Although most systems provide logging, log monitoring is only used to support troubleshooting, not security. Access to logs is not limited to key individuals, with the exception of the Common Customer application.

Monitoring can and has been enabled for specific users, but monitoring has not been conducted on shared IDs or network devices. Logs for these infrastructure systems are also not stored in a central logging facility, and are accessible to the ADH system administrators who have complete access to the logs and log settings for those systems.

Risk and Impact

Without monitoring of access there is limited visibility into the insider threat and the threat from a compromised ID. This presents a high risk that user IDs may be compromised or misused without detection.

Also, unauthorized changes to logs may occur if they are accessible by the administrators on those systems. Mistakes and unauthorized changes will not be detected, and a compromise of ADH systems and data can occur.

Without a robust log monitoring solution, ADH will have little to no knowledge of events causing breaches of information security on systems or across the organization. Likewise, ADH will have no evidence to trace back events to determine what happened, how it happened, and who performed the activity if central management and correlation is not available. Furthermore, IT personnel will be much less likely to be able to conduct an adequate forensic examination if they do not have experience in regularly reviewing system logs for evidence of attack.

ADH has many entities that connect directly to their intranet. However, it is difficult to determine if those entities operate secure networks. This exposure is especially significant as it's related to workstations in field offices or other State agencies for which ADH has less control. Compromise of the ADH network from a field office machine or computer on another State network is high.

With a lack of security verification as to other entities that are "trusted" within the ADH network, it is impossible to deny the high probability of compromise from those trusted network nodes.

Recommendations

Auditing of the network, application, server and desktop environments should be carried out using any logging and auditing capabilities that are currently available. Standards should be applied to what is logged on which types of systems and retained for as long as is possible (up to a year if possible). Additional logging for sensitive systems and sensitive data access should be provided.

ADH should also implement centralized log capture and monitoring capabilities to provide correlation of events across the enterprise and elimination of risk of access by local administrators.

These logs should be processed and reported against in an automated system if possible, and reviewed by independent personnel on a frequent and regular basis, following best practices for security log management and monitoring implementations. Security risks identified from these logs should be tracked and managed as directed by the ADH incident handling procedures.

Action

Windows AD logs are monitored and stored for a minimum 3 months. Firewall logs are monitored and stored for 6 month. Group policy is used for the updated on Windows OS products. Also GP is used to manage local control for our PC. PC are restarted by GP on every 20 days

2.3.4 Internet/Web Security

USDA Controls

Operating System Security:

To reduce risks, it is necessary to secure the operating system and physically secure the host system that runs the applications. This process is referred to as "hardening." The following procedures are used in the "hardening" process:

1. Eliminate unnecessary programs and services
2. Close all unused ports on the system
3. Change default file permission to be more restrictive
4. Enable verbose logging on the system (auditing)
5. Require a CMOS/PROM password
6. Disable file-sharing features
7. Adhere to password and user account policies and guidelines
8. Apply the most current system patches for the operating system.

The default installation of an OS will leave the system in an unsecured state. It is recommended that you follow the vendor's recommendation for securing your particular operating system. The ISSO should also provide the appropriate guidance for removing specific services and closing unused system ports.

Web Server Security:

One of the precautions to take when configuring a Web server is to never run the web service as a "root" or administrative user (super-user). The Web service should be run with the permissions of a normal user. This situation would prevent the escalation of privilege if the Web server were ever compromised. Also, do not configure the file system of the Web server (directories and files) to have write access for any users other than those internal users that require such access. Other precautions and secure configuration issues to consider when configuring a public Web server are:

1. The Web server should be on a separate local area network (DMZ) from other production systems
2. The Web server should never have a trust relationship with any other server that is not also an Internet-facing server or server on the same local network.
3. The Web server should be treated as an un-trusted host
4. The Web server should be dedicated to providing web services only
5. Compilers should not be installed on the Web server
6. All services not required by the Web server should be disabled
7. The latest vendor software should be used for Web server including all the latest hot fixes and patches.

CGI Scripts:

The following is a list of CGI best practices that should be implemented:

1. CGI Scripts should not be installed on a web server without the knowledge and consent of the ISSO.
2. The directory containing CGI scripts must have permissions of read/write/execute for owner and execute-only for group and others.
3. All CGI scripts should be owned by root or administrator.
4. All CGI scripts should have permissions of read/write/execute for owner and execute-only for group and others.
5. All backup copies of CGI scripts that are automatically generated should be removed from the system.
6. CGI scripts should not be available for FTP by users. The ISSO should document all CGI used on the web server.
7. Each CGI script should use a common directory for temporary files and once that task is completed, the temporary file will be deleted.
8. The ISSO should ensure that no CGI script source files exist in the web server document directories.
9. All CGI scripts should be centrally stored in the cgi-bin (or equivalent) directory.

Improper Input:

To limit improper input, the following activities should be performed:

1. Error checking should be performed on all input data.
2. Browser-dependant code, to include Active X, should not be allowed.
3. The following input should never be accepted by a CGI script:
 - a. Any cookie or special tag not created by your server.
 - b. Input that exceeds the maximum length of the defined variable.
 - c. Any non-alpha or non-numeric characters except special characters.
 - d. Values that are outside the defined scope of the expected value parameters.

Server Side Includes:

The capability to execute commands and scripts can pose a significant security exposure. Unless there is a valid business need, SSI should not be enabled on the web server.

Web Browser Security:

There should be a standard browser that has been approved by the ISSO for use within the EBT system environment. Due to the security holes in scripting languages such as JavaScript and Active X (Microsoft), it is recommended that all scripting languages not required for official EBT systems operation be disabled within the Web browsers.

Mobile Code:

Mobile code is the term for code obtained from remote systems, transmitted across a network, and executed on a local system. Mobile code also refers to Web-based code downloaded and run by the user's web browser.

Hostile mobile codes or executable content are completely different from the more traditional malicious codes, such as viruses and worms. Detection by standard antiviral software is more difficult. EBT users should be encouraged to avoid downloading, executing, or visiting sites that employ un-trusted mobile code. Some of the requirements for mobile code should include:

1. Mobile code should be digitally signed
2. Mobile code should only be accepted from trusted sources
3. EBT systems should be configured to block mobile code from un-trusted sources

4. Protections against malicious forms of mobile code shall be implemented in developed software and configured in COTS applications.

Findings

An effort to remove unnecessary or excess services on all systems has been implemented, but not reviewed by a professional security expert. ADH does not modify default operating systems to “harden” the operating systems, network devices or applications. File sharing support is enabled on some development servers.

ADH has one internal network on which development, test, and production servers are placed. Most production web servers, application servers, and databases are treated as trusted hosts are placed in this zone. All internal networks, including desktops and other State agencies have unobstructed access to this network and the systems that reside thereon.

Internet-facing web servers reside in a DMZ. Windows servers in the DMZ and those serving intranet applications have had trust relationships with the DIS Active Directory Forest, and the plan is to re-establish this AD trust and communication path.

CGI scripts are not used at ADH.

Due to the lack of proper security training of ADH development staff, adequate application security controls have not been applied to both internally developed applications and to the application that resides in the DMZ.

The development staff uses production data on development and test systems.

Risk and Impact

Disabling services and hardening servers does have an impact of not being able to quickly deploy or troubleshoot servers. However, hardened systems prevent many vulnerabilities from being exploited. If a platform has a vulnerability in SSH, for example, and SSH is enabled on a web server, the server is immediately vulnerable to attack, whereas if SSH was disabled, it would not be vulnerable.

System hardening guides and security standards more easily allow an organization to configure and deploy servers that do not have unnecessary or susceptible ports, agents, services, and permissions readily available.

Aggregating development, test, and production servers on one network creates a situation where servers are immediately and directly available to attack from peer systems. The ADH intranet is a trusted, but not secured network. ADH does use some access controls to separate the development systems, from test systems, and again from production systems. However, production systems in particular are susceptible to attack from peer systems on the same network.

Placing production application servers and database servers on the intranet creates a situation where the application sever and/or database is directly addressable on all ports from any device across the State network, including other State agencies and remote sites. Any of these sites may have wireless access points or open-ended connections to additional networks that allow further reach. ADH has

been struggling with a series of botnets due to this open architecture, which is an example of how malware can easily spread across a flat network.

Production systems contain sensitive personal information and benefit information. Once hardened, these systems will be more resistant to attack. Development and test servers are even more susceptible to attack because they are usually not hardened or have services enabled during development.

The use of production data on development and test systems puts this information at risk to exposure due to less strict security controls implemented on those systems. Placing these systems on the Intranet allows an easier attack and possible compromise of that sensitive data. These systems are commonly used as launch platforms for attacking the rest of the network, or for attacking other external targets.

Establishing trust relationships between servers in different security zones eliminates protections established by the boundaries of each security zone. A server compromised in an outer tier can then be used to launch an attack from a trusting system within a more secure zone.

There are risks in not having security involved throughout the SDLC. If security requirements and controls are not identified at the beginning of the SDLC, then it becomes riskier to evaluate the appropriate security mechanisms for that application as it nears readiness for deployment. For example, there may be flaws present such as not having password complexity and timeouts built into these applications that would expose ADH to vulnerabilities of not only the application, but its databases and the corporate network from insecure software. Remediation after the build phase often becomes prohibitively expensive or logistically difficult.

Recommendations

ADH information security architecture should be formally defined and fully integrated into ADH's SDLC, with other providers being a subcomponent to that process. ADH needs to take organizational steps and other measures to ensure that security risks are defined early in the development process, for local and distributed applications. There are security tasks that are required during every phase of the development life cycle. These tasks need to be developed and integrated within the SDLC. There are security risks at each of the major application milestones, and ADH needs to be able to make informed decisions regarding these security issues. The security staff should be educated as how to implement and maintain proper security controls in the SDLC.

ADH should segment its network into an n-tier server farm for production *intranet* systems, and another for production *Internet* systems. ADH should:

- 1) Isolate the development, test, and production systems into three separate environments, each with two to three tiers. All web servers in one tier, application servers in the second tier, and database servers in the third tier. If applications use fat clients or cannot be configured as three tier, then a reverse proxy or Citrix server should be used in the first tier.
- 2) Given existing budget constraints, ADH should use independent firewalls to separate and secure these environments at the perimeters. But minimally, ADH should use packet filtering between all tiered connections.
- 3) End point systems should not reside on the same network as web servers, applications, or databases.

Trust relationships should not remain between systems in different security zones, for example Internet to intranet, or development to test, or test to production.

When administrative or development access is necessary to these other environments, remote access should be encrypted and access logged and monitored for unauthorized events.

The development staff should investigate either a method to remove (e.g. “scrub”) real sensitive data from the development and test systems, or implement a method to create fake data that can be used for testing.

It is recommended that ADH develop policies, documentation, and procedures to implement software controls throughout the ADH infrastructure. A security officer or governance body should oversee this process and implementation.

Action

We have implemented parts of this section but do not agree with some of the recommendations. We see our development cycle safe because we do use non-patience data and data that has been scrub. We will continue to be diligence in our uses of Agency data and protect all patience data. Also our methods are peculiar to our data needs. We respectfully and carefully will care for our process and patience rights.

2.3.5 Network Security

USDA Controls

Firewalls:

The following firewall requirements should be implemented:

1. Firewalls that are accessible from the Internet are configured to detect intrusion attempts and issue an alert when an attack or attempt to bypass system security occurs.
2. EBT firewalls are configured to maintain audit records of all security relevant events. The audit logs are archived and maintained in accordance with applicable records retention requirements and security directives.
3. Firewall software is kept current with the installation of all security-related updates, fixes or modifications as soon as they are tested and approved.
4. EBT firewalls should be configured under the "default deny" concept. This means that, for a service or port to be activated, it must be approved specifically for use. By default, the use of any service or communications port without specific approval is denied.
5. Only the minimum set of firewall services necessary for business operations are enabled and only with the approval of the ISSO.
6. All unused firewall ports and services are disabled.
7. All publicly accessible servers are located in the firewall DMZ or in an area specifically configured to isolate these servers from the rest of the EBT infrastructure.
8. EBT firewalls filter incoming packets on the basis of Internet addresses to ensure that any packets with an internal source address, received from an external connection, are rejected.
9. EBT firewalls are located in controlled access areas.

Routers and Switches:

The following best practice solutions should be applied to all routers and switches throughout the EBT environment:

1. Access to EBT routers and switches is password-protected in accordance with FNS guidance.
2. Only the minimum set of router and switch services necessary for business operations is enabled and only with the approval of the ISSO.
3. All unused switch or router ports are disabled.
4. EBT routers and switches are configured to maintain audit records of all security-relevant events.
5. EBT router and switch software is kept current by installing all security related updates, fixes or modifications as soon as they are tested and approved for installation.
6. Any dial-up connection through EBT routers must be made in a way that is approved by the ISSO.

Findings

IBM's review of ADH network operations was conducted at a high level with assistance from ADH personnel. Overall the ADH network does use a single firewall at the perimeter, but could be configured to use the concepts of security zones for sensitive systems (see [Section 2.3.4](#)

Internet/Web Security). Intrusion detection is not used, and the firewall is not configured to alert or prevent access based on a detected attack. Firewall and network device security updates are only performed to address a bug or to obtain a new feature. Excess network or administrative ports are not disabled if they are not needed.

Risk and Impact

Intrusion attempts and attacks cannot be addressed if firewalls, network devices, or intrusion detection systems are configured to detect attacks. Attacks cannot be analyzed and forensics cannot be conducted if appropriate firewall and network audit logs are not maintained. Having too few or too many events captured can be equally detrimental, due to the time to filter excessive non-security related events or not having enough event detail for an investigation can result in undue risk to ADH.

All sensitive data eventually flows through the networking infrastructure, and as a result, a compromise of networking devices puts all systems on the network at risk of additional compromise. The first device available to an untrusted outsider on the Internet is a network router, then the outside firewall. Lack of adequate installation of critical patches to these critical network systems can lead to a complete compromise of the integrity and safety of the entire network.

Unused and administrative ports can be used as additional avenues of attack and penetration if not turned off, especially on the perimeter and where otherwise prudent. These settings must be verified on a regular schedule, otherwise there is no way to verify they are not being accidentally being made available for unauthorized access.

Recommendations

Intrusion detection should be deployed on Internet perimeter devices, other government office connections, and on network paths to un-trusted and unsecured portions of ADH's internal network (e.g. remote health offices). Serious consideration should be given to implementing network-based (NIDS) and host-based (HIDS) intrusion detection, given the distributed nature of the ADH intranet.

All firewall and network devices should follow the ADH Patch Management process. Patching of network devices is usually much less frequent than those of server and workstation operating systems, but when available they should be applied to remove the risk of compromise (especially at the perimeters of the network).

Encrypted communication should be used for network device management on all ADH controlled network segments instead of default administrative ports. On most network devices, this change should be trivial to implement. Unencrypted management should be disabled within each device and validated regularly as part of a formal vulnerability management program.

Logs for network devices and firewalls should be set to adequate levels of collection of vital information (as directed by ADH Network Security Policy). These logs should be monitored and maintained to reduce the risk of compromise and to help respond to audit requests and for root cause forensic analysis.

Due to the uncertain state of security within the ADH network environments, a vulnerability assessment should be performed to determine the relative security of the current environment.

Action

We have implemented all recommendations in this section.

2.3.6 Database Security

USDA Controls

To ensure data integrity, it is important to perform database administration correctly, regularly, and reliably. Some of the duties that will be performed to ensure data integrity are as follows:

1. Correct and successful physical backup of all database data
2. Correct and successful logical backup of all database data
3. Recovery operations
4. Database performance analysis
5. Enabling of auditing
6. Analysis of audit data

Database File Integrity:

To ensure the integrity of the database files the following procedures should be incorporated into the database security plan. These requirements should be derived from the EBT system-specific security policies.

1. Database COTS software should not be modified from its installation defaults to be more permissive.
2. All directories created by the installation of a RDBMS should not be modified to be more permissive.
3. Any groups created by the installation of a RDBMS should not be modified to be more inclusive.
4. Any file permissions created by the installation of a RDBMS should not be modified to be more permissive.
5. End users should never be allowed to change any directory names, file permissions, or group information associated with the database software.
6. All default and vendor installation accounts should be deleted from the system.

Database File Backup and Recovery:

A tested and verifiable backup strategy must be implemented for all EBT databases.

The DBA can create scripts or uses vendor-supplied scripts or utilities to perform backup and recovery operations. These scripts or utilities associated with backup and recovery should be available for review during the security review.

The database backup and recovery operations should be incorporated into the overall continuity of operations plans for the facility.

Findings

ADH is not encrypting sensitive personal information or electronic financial transactions. (This finding is not contrary to the EBT standard, but is a best practice and required by other regulatory standards.)

The SQL database server data is regularly copied to network shares for inclusion in the regular backup process. There is no encryption of this data on the network share, or while being stored on backup media.

Risk and Impact

Using unencrypted transmission across the network, between the web server, application server, and database, or encrypting the data in every location it may be stored can expose sensitive data to disclosure or tampering.

Implementing the use of encryption during transmission, while in storage, including backups, and integrating it as part of an application can be very expensive and time consuming. However, unauthorized disclosure of sensitive, personal or health related information can result in the expense of notification, fines, and the loss of privacy for the individuals whose data is compromised.

Recommendations

Encryption of sensitive personal information within the database, on the file system, within applications, and during transmission is recommended, but not mandatory for EBT. Encryption of sensitive personal information is a best practice regulatory requirement in many cases (especially for HIPAA), and may likely be a requirement in the future of EBT.

ADH should request legal interpretation of HIPAA and State privacy laws concerning the encryption of sensitive personal information in lieu of the type of data ADH stores or may store within their environment.

Action

We have not taken any Action. We are costing the price of full data encryption.

2.3.7 Virus Protection Controls

USDA Controls

All EBT systems should use antivirus (AV) utilities or programs to detect and remove viruses or other malicious code. The AV software must be kept current with the latest available virus signature files installed.

AV programs should be installed on workstations to detect and remove viruses in incoming and outgoing email messages and attachments, as well as actively scanning downloaded files from the Internet. Workstation and server disk drives should be routinely scanned for viruses.

The specific restrictions outlined below should be implemented in order to reduce the threat of viruses on EBT systems:

1. Traffic destined to inappropriate websites should not be allowed.
2. Only authorized software should be introduced on EBT systems.
3. All media should be scanned for viruses before introduction to an EBT system. This includes software/data from other activities and programs downloaded from the Internet.
4. Original software should not be issued to users, but should be copied for use within copyright agreements. At least one copy of the original software should be stored according to configuration management controls.

Findings

ADH utilizes anti-virus on all Windows systems, but not for the agency's single UNIX system.

Outbound Internet web traffic is filtered using a commercial product that is managed by the State agency DIS. ADH is investigating implementing and ADH-managed solution in the future.

Local users and even much of the IT staff do not have the authorization or ability to install unauthorized applications. This is controlled through ID access control and group policies.

Risk and Impact

UNIX systems have recently been determined to be the most vulnerable platform in 2010. Unpatched systems can be a target for attack, as well as act as a launch platform against the rest of ADH's systems environment. Along with a lack of anti-virus defense, UNIX systems are at the highest risk to compromise within an organization.

Recommendations

The agency's UNIX system should have anti-virus installed and running. One or even a handful of servers can be easily managed as a single device if the agency's existing antivirus management system is not capable of installing and managing an anti-virus agent on UNIX.

ADH should implement strict web filtering controls, and institute regular monitoring for compliance. If ADH cannot provide the necessary technology or skills to perform this, it should require it at the State level through agreements with DIS.

Action

We have blocked off the Unix system into its own area. No additional action required.

2.3.8 Penetration Testing

USDA Controls

Penetration testing is highly specialized field and requires staff knowledgeable in various testing methodologies, experienced in all levels of testing, and trained in the use of various testing tools. A systematic and analytical process must be used to evaluate computer resources for exploitable vulnerabilities. Penetration testing involves real world hacking techniques to identify security weaknesses and validate the overall security posture of a network.

As part of the security assessment for EBT systems, penetration testing should be incorporated to effectively evaluate the overall security posture of the network. The penetration test should be approached from a hacker's perspective. A combination of both commercial and freeware hacking tools should be used to scan the network to uncover any inherent vulnerabilities. Once all the vulnerabilities are found they should be documented, along with the mitigation strategies, to resolve each discovered vulnerability.

Penetration testing is accomplished in four phases:

1. Planning
2. Vulnerability Analysis
3. Attack Execution
4. Analysis and Reporting.

Findings

ADH has not conducted penetration testing in a while, and has not done so on a regular basis.

Risk and Impact

The most common and damaging attacks on the Internet today involve attacks on exposed vulnerable services, buffer overflows, cross-site scripting, and SQL injection. These are mostly application-related vulnerabilities, and ADH is unaware if these are possible to exploit by unauthorized inside or outside entities without implementing penetration testing to verify the level of risk.

Recommendations

Given ADH's web-centric application environment, penetration tests should be conducted at least annually against the agency's most sensitive applications.

The focus of any penetration test should be the access to customer sensitive data or health related information.

Action

We have performed a penetration test and found no problems. No additional testing.

2.4 EBT SPECIFIC CONTROLS

Comments

This assessment has included the requirements for EBT Specific Controls for completeness, but cannot evaluate these controls before an EBT system has completed a design stage.

The previous three domains address security concepts and controls that are required within an environment that supports an EBT system. The controls in these prior sections can apply generally (in most cases) to any secure environment.

The controls in this section are intended to be specific to an EBT system and cannot be evaluated in the absence of an EBT system or system design.

IBM recommends using the *FNS-EBTS Security Controls Handbook* guidance and controls matrix to derive the security design requirements for the EBT system. In the event ADH chooses to use an external provider, the provider must adhere to the requirements in the handbook; ADH would then need to create a contract that requires compliance with the standard and to oversee the provider's compliance with these standards.

2.4.1 EBT Access Card Security

USDA Controls

Security issues associated with EBT access cards have been raised due to the high frequency of maintenance activities associated with them. Access cards are continually issued, activated, replaced, and destroyed. Therefore, the potential for fraud exists at many points in the life cycle of the cards. To mitigate the risk of fraud, several security measures should be incorporated into the cards.

1. **Magnetic Stripe Card Security** - includes requirements for conformance to International Organization for Standardization (ISO) standards, and policies for card inventory management, card activation and deactivation, PIN mailings, and card lifecycle.
2. **Smart Card Security** - includes requirements for the operating system, the ability to disable and enable chips, key management, expiration dates, encryption, biometrics verification and security for multi-application cards.
3. **Hybrid Card Security** - includes the same requirements for magnetic stripe cards and smart cards. It also includes controls to prevent security loopholes such as the ability to use the magnetic stripe to access benefits when the smart chip is not functional.
4. **Optical Card Security** - includes requirements for the confidentiality of data stored on optical cards, the use of data encryption, and the use of anti-counterfeit features.

2.4.2 POS Terminal and ATM Security

USDA Controls

Recipients gain access to their benefits through POS terminals and ATMs. Benefit transactions can be performed through on-line processing, off-line processing, and manual processing.

1. **On-line Processing** - On-line processing uses a central processor to verify PINs and authorize transactions. Requirements include cashier ID and password verification, settlement controls, integrity of transmitted data, and on-line biometric verification.
2. **Off-line Processing** - Off-line processing performs PIN verification and transaction authorization at the point-of-sale. Requirements for this security element may include mutual authentication between the smart card and the POS terminal, non-repudiation controls for transactions, and off-line biometric verification.
3. **Manual Processing** - refers to backup procedures for either on-line or off-line processing. It includes paper vouchers and manual entries. Security requirements include policies and controls for sales vouchers, suspense accounts, and settlement.

APPENDIX A

Interview List

IBM security consultants interviewed the following ADH employees. We wish to thank everyone who participated in the project, who provided valuable information which supported our efforts.

Contact Name	Area of Responsibility
Jerry Pack	Chief Information Officer
Warren Bankson	Information Systems Coordinator
Xavier Heard	Human Resources Director
Candy Wright	Help Desk
Bert Wells	Information Systems Coordinator (EBT)
Francis St. Germaine	Computer Support Manager (Desktop Support)
Robert Pelton	Information Systems Coordinator (Application Development)

Documentation List

IBM security consultants reviewed documents including process diagrams, application inventories, and project lists. The list of documentation reviewed, by file name is as follows:

Document File Name
2010_08_13_22_45_32 (EBT Locations).pdf (<i>scanned paper document</i>)
2010_08_13_22_45_44 (ADH Org Chart).pdf (<i>scanned paper document</i>)
ADH APPROPRIATE USE OF EMAIL & INTERNET.doc
ADH INFORMATION SYSTEMS PASSWORD REQUIREMENTS.doc
ADH INTERNET FILTERING.doc
ADH IT SECURITY TRAINING REQS.doc
ADH REMOTE ACCESS POLICY.doc
BLACKBERRY SECURITY STANDARD.doc
DISPOSAL OF SURPLUS COMPUTER EQUIPMENT.doc
EMAIL USAGE POLICY.doc
Information Security Policy for Department of Health - draft v1.doc
INFORMATION SYSTEMS DEVELOPMENT.doc
INFORMATION SYSTEMS SECURITY ACCESS.doc
VISIO NETWORK DIAGRAMS:
10000 foot drawing 9-16-08 .vsd
ADH-Ihu Sample.vsd
agency DMZ.vsd
video-conf no ip address.vsd

HEALTH – Schedule #3

Date: 10/30/2012

Schedule ID : HEALTH

SUMMARY OF SERVICES

Selected Services
Replacement Recovery System
Primary Recovery Facility
Alternate Recovery Facility
Mobile Date Center
Subscriber Facility
Network

Total Monthly Fee: \$1,097.28

Term: 24 Months

Qty	Mobile. 10 Customer Configuration Ref: Health	Declaration Fee	Daily Usage Fee ⁴
		\$0	\$1,250
4	x86 Server (w/ Monitor, Keyboard, Mouse)		
	Health		
2	Intel Dual-Core 3.4 GHz Xeon CPU (EMT64, VT)		
4	GB Memory		
292	GB Internal Disk		
1	DVD-RW Drive		
1	Ethernet 10/100/1000 Mbps Port		
1	x86 Server (w/ Monitor, Keyboard, Mouse)		
	Health		
2	Intel Dual-Core 3.4 GHz Xeon CPU (EMT64, VT)		
8	GB Memory		
292	GB Internal Disk		
1	DVD-RW Drive		
1	Ethernet 10/100/1000 Mbps Port		
1	x86 Server (w/ Monitor, Keyboard, Mouse)		
	Health		
2	Intel Dual-Core 3.4 GHz Xeon CPU (EMT64, VT)		
16	GB Memory		
1168	GB Internal Disk		
1	DVD-RW Drive		
1	Ethernet 10/100/1000 Mbps Port		
1	Fiber Channel Port		
1	Cisco ASA 5550 Adaptive Security Appliance		
4096	MB DRAM		
8	10/100/1000 Ethernet Port		
1	Cisco ASA 5540 Adaptive Security Appliance		
2048	MB DRAM		
4	10/100/1000 Ethernet Port		
1	F5 Networks Big IP 6400 Traffic Manager		
16	10/100/1000 Ethernet Port		
4096	MB DRAM		
1	SSL Accelerator 1000 TPS		
48	1000Base-SX MMF Switched Ethernet Port		
150	10/100/1000Base-TX Switched Ethernet Port		

SUNGARD PROPRIETARY AND CONFIDENTIAL

This page contains and describes confidential information. It is intended for the use of the person named in the header. If you are not the named person, you should not disseminate, distribute or copy this page. If you are not the named person, you should not disseminate, distribute or copy this page. If you are not the named person, you should not disseminate, distribute or copy this page.

FOOTNOTES

1. Customer acknowledges that, subject to then current availability, the 1.44MB floppy diskette drive in this configuration may be replaced with a DVD drive by SunGard.
2. Only available at the Primary Recovery Facility for Tests or in the event of a Disaster.
3. Daily Usage Fees during a Disaster will begin on day 1.
4. Daily Usage Fees during a Disaster will begin on day 31.
5. If a Declaration Fee of equal or greater value is charged in association with a Center-Based or Mobile Configuration defined on this Schedule, then the Declaration Fee for the applicable Network Services will be deemed included in such fee.

SUNGARD PROPRIETARY AND CONFIDENTIAL

The fees, services and other items described above are for informational purposes only. They are not intended for an offer or contract and are not binding upon SunGard. Taxes are not included in the estimated fees.

Version: 03-24-2012