Inter Tribal Council of Arizona
STARS Project

WIC Automation System
Deliverable #8D -
Security Plan – Final

Contract # 04-06

Submitted On:
January 10, 2005

Starling Consulting, Inc.
711 S. Capitol Way, Suite 301
Olympia, WA 98501

STARLING CONSULTING

Security Plan
Table of Contents

Introduction

The Security Plan for the Inter Tribal Council of Arizona (ITCA) provides a detailed description of the physical security, inventory and configuration control, data security, telecommunications security, personnel security, and operating procedures.

Security is addressed at the physical, network, operating system, and application levels in this document.

Because ITCA will assume operations responsibility for STARS and because ITCA is hosting the central processing site, SCI has identified many of the security requirements as recommendations. Both ITCA and SCI are committed to minimizing the overall security risks to the project, while balancing the cost, functionality, performance, and reliability of the Shared Tribal Automated Reporting System (STARS).

The STARS Security Plan consists of these major sections:

Risk and Vulnerability Analysis
This section addresses realistic and foreseeable security risks for hardware, data and sensitive supplies for the project.

General Approach to Security
This section describes common approaches to protecting all equipment, data, and supplies.

Security at the Central Processing Site
The Central Processing Site houses a copy of the consolidated database and the systems necessary to support synchronization and reporting. This section describes the procedures necessary to protect client data and ensure continued access to the synchronization functions.

Security at the WIC Central Office
Central Office staff have access to several applications that control the overall system functionality. This section addresses the security requirements and implementation strategy to ensure that the application is securely maintained.

Security at WIC Clinic Sites
All ITCA WIC clinics across the State of Arizona will have equipment, sensitive consumable supplies (check stock and MICR printers), and locally hosted client data. This section describes the measures that SCI and ITCA will implement to secure these system components. Security requirements are addressed for physical, data, application, local network, client confidentiality, and WIC checks at WIC clinic sites.

Application Security
The STARS application uses individual user logons and security groups to provide access to the application at a screen level. This section includes a description of role-based application security features and a plan for facilitation of user expert specification of roles, system access by role, and assignment of staff to roles. It also includes a security matrix that shows staff access to the application by screen and by staff role.

SCI has identified the following critical success factors for the project, in regard to security:

- SCI, ITCA, and Local Agencies will work in partnership to protect the STARS systems and data, ensuring the confidentiality, integrity and accessibility of the STARS data.

- Security requirements will be examined at several levels, including physical, network, operating system, and application levels. It does little good to have strong network security if there is no physical security in place.

- The project stakeholders realize that a robust security response is dynamic, and may change if new risks are identified.

- Both ITCA and SCI remain committed to providing appropriate security, balancing overall costs with protection of critical resources and data.

- ITCA and clinic end users recognize their significant role in security management, particularly in regard to protection of confidential client data, equipment, and sensitive consumable supplies.

- Project staff use best practices for security, including regular anti-virus updates, vigilant monitoring of log files, strong password policies, and controlling access to systems and supplies.

Risk and Vulnerability Analysis

Types of Security Risks

The STARS Project is vulnerable to security risks similar to other information systems containing personally identifiable client information. Deliberate or inadvertent actions that impact the confidentiality, integrity or accessibility of the data or applications are security threats.

- **Unauthorized disclosure of data**
  Unauthorized access to datasets, excessive proliferation of datasets, and deliberate or unintentional breaching of security to networks, workstations and dial-in systems.

- **Modification or destruction of data, applications or operating systems**
  Corruption of data, applications or operating systems due to deliberate or inadvertent actions, programming errors, or power outages, and contamination by viruses or worms.

- **Unauthorized access to facilities**
  Breaching physical access controls to server locations, building entrances, theft or destruction of equipment and sensitive inventory (e.g., magnetic toner, blank check stock).

- **Denial of service**
  Deliberate or inadvertent loss of service to Central Processing Site servers, clinic servers, or networks.

Vulnerability Assessment

Based on actual operational assessments of the security risks for the WIC Automation Projects in Washington, Puerto Rico, and Kansas, SCI rates the security risks for STARS as low to medium, as shown below. The risk rating is a subjective reference and based upon the security measures implemented for the STARS system. Low risk means that the chances of the threat occurring is less than 1%, Medium risk means that the chance of the threat occurring is less than 10%.

Threats	Security Risk Rating
Unauthorized Disclosure of Data	Medium
Modification or Destruction of Data	Low
Unauthorized Access to Facilities	Medium
Denial of Service	Low

Data disclosures can range from having a client assessment printout visible on a WIC staff member's desk while another client is present, to having a local clinic database copied to removable media, to a full disclosure of the central database.

Data destruction or modification that involves more than one client typically requires full administrative access to the database server. SCI recommends that ITCA operations staff log administrative access and make daily backups of the consolidated database. The process of synchronization backs up local clinic data to the consolidated database at least once per day. If a clinic database is destroyed, operations staff will re-extract a copy of the local clinic database from the consolidated site. At most, the clinic will lose changes made since the last synchronization process. Other processes should be put in place to minimize the potential for loss of data. For example, the hardware specification calls for servers with dual hard drives. The second hard drive acts as a mirror to the first and can be used to restore data if the first drive fails. Clinics with broadband connections can be configured to replicate more frequently than once per day. In addition, clinic staff can easily initiate replication any time they wish.

Facility access is controlled by the WIC Central Office or Local Agency staff. There will be some variability among clinics in terms of their physical security and access to facilities. At the Central Processing Site (CPS). SCI recommends that ITCA place appropriate controls on access to the CPS in order to prevent unauthorized access. In the clinics, SCI recommends placement of the server, check printer, and sensitive supplies in an area that is controlled and monitored, and outside the normal client flow. SCI will also provide any additional facilities recommendations for clinics as identified during the on-site survey visits.

Denial of service risks are most likely at the Central Processing Site. Normal clinic services operate within the local network, and do not depend on the Internet. However, clinics synchronize data nightly via e-mail, and that process is subject to interruption if the e-mail server is flooded with nonsense packets designed to interrupt services. SCI recommends the use of dynamic packet filtering at the router/firewall level to drop excessive packets from unauthorized systems. SCI recommends configuring the e-mail server to reduce or eliminate vulnerabilities to mail relaying and other tactics that compromise e-mail services.

Security risks are related to the facilities in which STARS operates. For example, the security threat "Unauthorized Access to Facilities" may be higher in a small clinic without a dedicated, locked data center than at the Central Processing Site, where access to the data center is controlled and managed by ITCA operations staff. The following table displays SCI's overall estimated level of risk for each type of facility.

Facility	Facility Risk
Central Processor Site	Low
Central WIC Office	Low
WIC Clinics	Medium

The distributed architecture further reduces the security risk by providing localized services at each clinic, rather than relying on a centralized service model with a single identifiable target. If one clinic is targeted, other clinics are not affected. If the Central Processing Site is compromised via a denial of service attack, clinics can operate independently until the security issue is resolved.

General Approach to Security

The STARS system employs multiple layers of security to minimize the overall risk to the system and data, at the physical, network, operating system, application and database level.

SCI recommends that ITCA adopt industry best practices to minimize the security risk to the STARS system. Below is an overview of the methods used to protect STARS from deliberate or inadvertent security risks.

Layer	Security Practices Implemented
Physical	• Control physical access to the servers. • Limit and manage copies of the databases on removable media.
Network	• Use firewalls and routers to control access to the CPS based on source IP address and destination port. • Monitor logs for unusual activity. • Implement dynamic filtering to reduce risk of denial of service attacks. • Use software-based firewall on small WIC clinic networks which don't already have a firewall in place.
Operating System	• Apply latest service packs, security patches, and virus protection software in a timely manner. • Disable all unnecessary services. • Enable strong password policies. • Limit administrative access to system. • Install and automatically update anti-virus protection. • Use NTFS security to protect OS, applications, and data. • Limit network shares and ensure just enough access is granted. • Log failed access attempts, monitor CPS server logs regularly.
Application	• Require unique logon for all STARS application users. • Enable strong application password policies. • Enable access on a screen-by-screen basis using application groups and security roles.
Database	• Enable strong database password policies. • Allow only administrators to access the database directly (except for limited direct access to an ad-hoc reports server). • Allow only the application to communicate directly with the database. • Remove default group access privileges. • Log administrative access to database. • Make daily backups of the central database server.

Security at the Central Processor Site

Physical Security

ITCA operations staff will control access to the data center where WIC servers are operating. SCI recommends that ITCA operations staff monitor and log access to the facility, and periodically conduct a security review of the facility to identify changing risk exposure. Risks to assess include natural disaster (i.e. lightning strike, fire, earthquake, etc.), burglary or vandalism of the site, overheating of the facility due to loss of air-conditioning, and unauthorized access by visitors.

Backup Data Storage

Back-up tapes should be stored both on location at the Central Processing Site, and off-site at a location to be determined by ITCA. Tapes in both locations should be properly protected. ITCA IT staff should store the backup tapes in a secure manner, for both on-site and off-site locations. Off-site backup should be performed at least weekly.

Staging and Deployment of New Central Processing Site Equipment

ITCA is responsible for providing hardware for the STARS project. ITCA operations staff are responsible for securing CPS servers. ITCA is responsible for controlling access to the staging and deployment facility, ensuring adequate inventory records are kept for the project, and protecting equipment and parts from unauthorized use.

SCI recommends that ITCA inventory and tag all equipment upon receipt, in accordance with ITCA inventory policies and procedures. A log should be kept of any equipment removed from the facility, including the tag number of the equipment, its description, the person removing the equipment, and its destination.

Data Security

Data Security protects against risks of unauthorized disclosure of data, modification, or destruction of data and unavailability of data.

The only direct access to the STARS data on the consolidated database is by operations staff. During the pilot test and rollout SCI operations staff will remotely manage the CPS using remote access to CPS servers. After the transition of operations responsibility to ITCA, ITCA operations staff may grant additional remote access to SCI for the purpose of providing third tier operations support. Changes made to standard reference data in the consolidated database will be synchronized with all clinic servers when the clinic server initiates the synchronization process.

Local clinics will synchronize periodically with the CPS. SCI recommends that automatic synchronization be configured for each clinic based on that clinic's telecommunication access. The general goal is to have each clinic synchronize at least once per day. The synchronization process

uses SQL Remote and an SMTP (Simple Mail Transfer Protocol) e-mail server. SQL Remote synchronization packets are encoded by the synchronization agent before transmission to protect the data in transit. Synchronization packets contain a coded, internal database identifier for both the publishing and the subscribing database. This ensures that only the intended subscriber database can read the synchronization packet. In addition, the subscriber database accepts synchronization packets only from the publishing database specified during the configuration process. It is not possible to apply synchronization packets to any other database other than the one it was intended for, even if the structure and the data is the same. See the section titled: Telecommunications Security for more information on securing the data in transit.

Application Security

SCI will periodically provide new versions of STARS applications to ITCA operations staff for deployment. ITCA operations staff will install updated STARS applications, utilities or commercial application updates on the CPS servers. SCI recommends that ITCA conduct an acceptance test for all software releases in a test environment prior to installing new STARS application releases.

The STARS system uses SMTP to transfer synchronization packets between the CPS and the local clinic servers. The SMTP synchronization server will be configured to allow only machine-to-machine communication using SCI's Message Application Protocol Interface (MAPI) utility. The STARS system will not use Microsoft Outlook or any other commercially available e-mail client, nor will any e-mail addresses be stored in any form of an electronic address book. SCI will configure the Exchange 2000 server to send and receive e-mails from only the clinic servers, the Central Office, and the CPS. No human-generated e-mail will be allowed on the synchronization server. SCI will configure the Exchange 2000 server to reject anonymous mail relay requests so that it cannot be used by other individuals or processes. SCI will follow Microsoft's best practices recommendations for securely configuring the server, and will ensure that all application security patches are installed on the system.

SCI will use Windows 2000 Terminal Server for remote access from the SCI Operations Center to the CPS and Central Office server. All remote access sessions will be protected by an encryption process determined by ITCA and SCI. ITCA operations staff will have ultimate authority over remote access to the central processing site.

Virus Protection

It is the responsibility of ITCA to install and maintain virus protection software on all Central Processing Site servers and user workstations. SCI assumes that ITCA will use mainstream virus protection systems such as Norton Anti-Virus Corporate Edition or similar competing products.

Network Security

Network security consists of protecting and monitoring any network entry points and ensuring that routers, firewalls and other network devices are configured properly to prohibit unauthorized entry or use of network services.

ITCA is responsible for network security at the Central Processing Site.

Telecommunications Security

Telecommunications security measures protect against unauthorized disclosure of data, modification or destruction of data, and unavailability of services. Clinic servers will synchronize data with the Central Processing Site (using the SMTP protocol) by accessing the communications server in the CPS.

ITCA approved encryption software should be used to encrypt any confidential STARS data transmitted to or from the Central Processor Site over public communications facilities. This includes synchronization data transmitted to and from the clinics via SMTP. The encryption level should be 128-bit or greater.

Remote access to Local Agency and Central Office WIC servers by SCI Operations staff will be protected by logon and strong password access.

Security at the WIC Central Office

WIC Central Office staff should follow the same measures outlined in the section titled; General Approach to Security regarding physical, network, operating system, and application levels of security. Although the WIC Central Office will be co-located in the same building with the Central Processing Site, SCI recommends that appropriate measures be taken by ITCA operations staff to limit direct access to the central processing site by ITCA users.

Access Control

At the Central Office, ITCA Operations staff have access to utilities that configure and control user access to STARS. Central office users issue compliance checks, manage pricing, and other tasks that have far-reaching impact on all WIC clinics. The following additional steps are necessary to protect the STARS system specifically at the Central Office.

Central Office application access will be controlled using role-based application security. Only staff who are authorized to perform certain functions will be granted access to each specific application. The ITCA WIC Director approves access to Central Office applications, and ITCA operations staff will manage the user accounts. The creation of new user accounts and the inactivation of existing accounts will be completed by ITCA operations staff, and will be directed by the ITCA WIC Director or her designee. The WIC Director or her designee will assign each user account to specific security groups and assign access privileges to specific Central Office applications.

Virus Protection

It is the responsibility of ITCA to install and maintain virus protection software on all Central Office workstations that access STARS data.

Application Security

Central Office staff must enter an account name and password before gaining access to the any of the Central Office applications. Operations staff will assign authorized individuals access to specific applications based on written or verbal requests from the ITCA WIC Director or her designee.

Central Office staff are assigned to a particular security group by operations staff, which regulates their access to the applications on a screen-by-screen basis. See Appendices A-K Security Matrix Plan for a detailed listing of recommended groups and access privileges by application and menu item. Access levels for each user ID shall be limited to the screens necessary to fulfill that user's responsibilities. Each user shall have a unique user ID assigned. User IDs may not be shared under any circumstances. The STARS system has an administrative report that shows all users authorized to perform specific functions.

Passwords must be entered manually; sign on scripts that include passwords are prohibited. Application passwords must be at least five characters long, must contain at least one letter and one

number or character. The STARS application will force a password change every 60 days, and must be replaced with a new password dissimilar from the previous password.

A security timeout feature is included in all Central Office applications. Once a certain time period has passed without a key press or mouse click, a security window pops up and the user is forced to re-enter their password before being able to continue. If they are unable to re-enter their password, they are logged off the application. The time period is configurable by ITCA's Database Administrator.

Data Security

Individuals with access to client data shall be trained in confidentiality requirements and steps to protect unauthorized disclosure. Such users shall be required to orient their monitors so passers by cannot see data, and to exit the STARS application completely whenever leaving their desk.

Reporting

Certain Central Office staff will have access to an ad-hoc report service. Those staff will be given database accounts that provide read-only access to most tables, with the exception of security tables, where there will be no access granted. Those staff should have skills sufficient to create queries and interpret their results. They should also be briefed in the database structure of the STARS system. The ITCA database administrator (DBA) will authorize individual access to the ad-hoc report service. ITCA operations staff will manage user access for the ad-hoc report server.

Central Office staff will have access to additional reports for statewide reporting. Access to the statewide reports is controlled in the same manner as any other screen in the STARS system. Access to menu items is assigned to particular security groups. Staff are placed in security groups and are automatically granted access to the menu items allowed for that group.

WIC Checks

A MICR-enabled printer will be available for use at the Central Office to print checks in the event of the catastrophic loss of a WIC clinic (by tornado, flood, fire, etc.) and to print compliance-buy checks.

The MICR-enabled printers have built in security features:

- The MICR font may only be printed with special command codes. Access to the Programmer's Manual which describes these codes is limited to the SCI lead developer.
- Each print command for a MICR document is constrained to a maximum number of characters.
- The printer is never left in "MICR mode" at the end of a print command.

These security features are designed to restrict check printing capability to only systems running the STARS application.

To minimize the risk of fraudulent printing of checks, the following measures should be implemented:

- The MICR Programmer's Manual will always be kept in a locked, secure area.
- Source code that enables the WIC Automation Project application to print WIC checks will be kept in a secure directory. Source code will never be distributed to clinics.
- MICR toner cartridges will be carefully regulated. They will be distributed in limited quantities to replace exhausted cartridges at the Central Office or clinic sites. Operations staff should monitor use of both toner and check stock and inform Central Office staff of excessive use beyond projected volumes based on clinic caseload. Clinics should also carefully inventory and monitor supplies.
- SCI recommends that MICR printers used in the training labs or test facilities will be removed upon completion of the training and testing.
- SCI recommends that MICR printers at the local clinics and the central office will be positioned away from the flow of traffic and in a well-monitored location.

Security at WIC Clinics

WIC clinic staff should follow the same measures outlined in the section titled: General Approach to Security regarding physical, network, operating system, and application levels of security.

Physical Site

Clinic staff will be required to exercise adequate physical security of STARS equipment, data and supplies. Servers that do not double as workstations will be kept in a separate, locked room where possible. Physical security may be the subject of a written agreement with a Local Agency.

Buildings containing STARS equipment should be locked and secured outside of regular business hours.

Staging and Deployment of New Local Agency Equipment

ITCA is responsible for providing hardware for the STARS project. ITCA Operations staff are responsible for securing and inventorying servers, workstations, notebooks, and check printers awaiting shipment to WIC sites. ITCA is responsible for controlling access to the staging and deployment facility, ensuring adequate inventory records are kept for the project, and protecting equipment and parts from unauthorized use.

ITCA will inventory and tag all equipment upon receipt, in accordance with ITCA inventory policies and procedures. A log will be kept of any equipment removed from the facility, including the tag number of the equipment, its description, the person removing the equipment, and its destination.

SCI will configure and test the equipment that ITCA installs at local WIC clinics during the initial rollout of STARS. ITCA will transfer custody of the equipment to clinic staff following ITCA policy and procedures.

Inventory Control

Magnetic toner cartridges and check stock should be stored in a locked secure location. ITCA Operations staff will dispatch supplies to the local clinics. They will be distributed in limited quantities to replace exhausted cartridges and check stock at the local clinics.

Portable Equipment

If finances allow, portable notebook computers should be fitted with locks designed for notebooks, and secured to a desk whenever possible. Unattended notebooks should be locked to a desk or similar immovable object, or stored in a locked cabinet or room. Notebook computers should not be left in vehicles unless locked in the trunk out of view. Notebook computers should be protected from excessive heat and cold and from unnecessary bumps and drops. Portable MICR printers should be secured and protected in the same manner as notebooks.

Data Security and Confidentiality

The STARS database at each local clinic will hold a copy of all client data for that clinic's caseload. It is imperative that access to client data be closely managed to conform to State, Federal, and contractual requirements for confidentiality.

As part of the implementation training, all clinic personnel will be trained in confidentiality requirements and steps to protect unauthorized disclosure. Users will be trained to orient their monitors so passers by cannot see data, and to exit STARS completely whenever leaving their desk.

The STARS system tracks the staff ID associated with each client contact, including issuance of food instruments and certifications.

No direct access to the local clinic database will be allowed. Only the ITCA DBA will directly access the local database, and only when necessary to resolve a problem.

Virus Protection

All servers, workstations, and notebooks used for the STARS system should have up-to-date virus protection software installed. The software should be configured to automatically update itself on a regular basis.

ITCA Operations staff will install and maintain virus protection software on all clinic workstations connected to the STARS system that are not managed by Local Agency IT staff. The virus protection software should be configured to automatically update itself on a regular basis.

Users should be trained to follow established policies prohibiting downloading and/or installing unauthorized applications or data onto STARS computers. Staff should comply with ITCA and local agency policies regarding downloading approved applications and virus screening.

SCI assumes that some local agencies are supported by their own IT staff who have local standards for maintenance of virus protection software at their clinics. For local agencies without these local service providers, SCI recommends that ITCA provide anti-virus software for all servers, workstations and notebooks purchased for the project.

Application Security

WIC staff must enter an account name and password before gaining access to the Client Services application. The names, passwords and security group assignments will be maintained by ITCA operations staff. See Appendices A-K Security Matrix Plan for a detailed listing of recommended groups and access privileges by application and menu item. Access levels for each user ID shall be limited to the screens necessary to fulfill that user's responsibilities. Each user shall have a unique

user ID assigned. User IDs may not be shared under any circumstances. The STARS system has an administrative report that shows all users authorized to perform specific functions.

The application security controls are flexible enough to accommodate staff with multiple roles, which is typical for small clinics. ITCA operations staff will create security groups and assign screen access permissions to each security group. As an example, operations staff may create a security group called "Clerk/Administrator," which could be used by small clinics where the clerk has more responsibility and authority than normal. Ninety-five percent of the staff will be served by a few basic security roles, like RD or local administrator. The remaining 5% can have custom groups established to address the local clinic access requirements.

Passwords must be entered manually; sign on scripts that include passwords are prohibited. Passwords must be at least five characters long, must contain at least one letter and one number or character. The STARS application will force a password change every 60 days, and must be replaced with a new password dissimilar from the previous password. SCI recommends that users be trained in best practices for security during their training sessions.

ITCA operations staff will create new user accounts, be able to change passwords, and inactivate existing accounts for the STARS application. This process will ensure that each STARS user has only one valid user account. Operations staff will then assign the user to specific security groups and assign access privileges for the user. The STARS system will require that users change the temporary password at the time they first log onto the system.

A security timeout feature is included in the Client Services application. Once a certain time period has passed without a key press or mouse click, a security window pops up and the user is forced to re-enter their password before being able to continue. If they are unable to re-enter their password, they are logged off the application. The time period is configurable.

Network Security

WIC staff must enter an account name and password to gain access to the Local Area Network at the clinic.

LAN user accounts and access privileges will be managed locally. Clinics which have existing networks and local technical support are responsible for managing their own local network security.

SCI assumes that Local Agency clinics have established networks, varying degree of Internet access, and varying levels of local IT support staff (either through the tribal agency or ITCA). SCI will coordinate with designated local or ITCA IT staff to recommend network security improvements where necessary.

Internet Browser Access and Security Risk

At any Local Agency clinics where users can access the Internet, we assume that Local Agency staff will implement virus protection and other software to prevent security breaches and interruption of WIC automation services. SCI recommends that access to the Internet by local agency staff (via a browser) be limited and/or carefully monitored to limit the exposure to viruses and worms that could affect local STARS database and application services.

WIC Checks

Blank check stock will be stored at WIC clinics. Also, MICR-enabled printers will be used to print checks on a daily basis. Finally, a supply of MICR toner cartridges will be stored at WIC clinics.

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

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

- The MICR enabled printers should be closely monitored. The printer should be placed in a location removed from waiting areas and high traffic areas where possible.

- MICR toner cartridges and blank check stock should be securely stored and accounted for.

Application Security Groups

ITCA operations staff will grant permission for access to the STARS applications on the basis of each users roles and responsibilities.

When a new staff member starts, ITCA operations staff will add the user to the global user table. If the new staff member is a local agency staff, operations staff will associate the new staff member with the local clinic, and assign the new staff member to a particular group (Clerk, Nutritionist, etc.). The new staff member will be able to log in and use the STARS application at that clinic, with the permissions assigned to the designated group.

Each security group grants a certain type of access to a set of menu items in each application. For each menu item in a STARS application, a member of the security group will have one of three types of access:

- Full access – user group will have full access to all functionality of the screen or window.
- Read only – user group will have ability to read but to not write to the screen or window.
- Not Visible – menu item will not appear for this user group.

The Appendices to this deliverable contain the security matrix by application. These are recommended security levels based on previous SCI WIC projects. The SCI requirements analyst will work with ITCA user experts during requirements review to customize security groups for all STARS applications.

Security Matrix Plan Appendix

The appendices show initial suggestions for user groups and access permissions based on previous SCI WIC projects. They are not intended to be definitive security rules. ITCA WIC has the ability to add new groups and make any changes to access permissions at any point. User groups and access permissions specific to ITCA WIC will be defined during Requirements Review. These appendices will be revised based on the agreements made during Requirements Review.

Appendix A. Banking Management

Appendix B. Vendor Management

Appendix C. State Client Info

Appendix D. Investigation Management

Appendix E. Participation & Financial Reports

Appendix F. Checks Management

Appendix G. Clinic Management

Appendix H. Food Package Management

Appendix I. Breastfeeding Monitor Reports

Appendix J. Infant Formula Rebate

Appendix K. Client Services Application