



SECURITY PLAN

PRESENTED TO

SPIRIT

FOR THE

WIC SPIRIT AUTOMATION PROJECT

May 19, 2005

**Task # 1
Deliverable # 9**

1. SECURITY PLANNING AND ADMINISTRATION	3
1.1. SYSTEM ACCESS CONTROL	3
1.1.1. <i>Create Role Profiles</i>	4
1.1.2. <i>Create User Profiles</i>	5
1.1.3. <i>Password Development</i>	5
1.2. SEPARATION OF DUTIES	6
1.3. PERFORMING BACKUPS	7
2. SYSTEM AND DATA INTEGRITY	8
2.1. SYSTEM INTEGRITY	8
2.2. DATA INTEGRITY	8
2.2.1. <i>Conversion</i>	8
2.2.2. <i>Implementation</i>	9
2.3. OPERATIONS.....	9
2.3.1. <i>Local Clinics</i>	9
3. SYSTEM SECURITY	11
3.1. CONVERSION	11
3.2. IMPLEMENTATION	11
3.3. OPERATIONS.....	12
3.3.1. <i>System Security</i>	12
4. RECOMMENDATIONS FOR NON-COMPUTER RELATED TASKS	14
4.1. CHECK STOCK	14
4.2. COMPLIANCE BUY CHECKS	14
4.3. PRINTERS.....	14
4.4. MONITORING POSITIONING TO CUSTOMER VIEW	14

Security Plan

This Security Plan will address various security issues related to ensuring the accuracy, integrity, authenticity, and confidentiality of data and resources for SPIRIT WIC. It will address issues such as assignment of user accounts, definition of system responsibility levels, development and format of passwords, frequency of password changes, and maintaining hardware.

The Security plan will address measures built into the system to detect and prevent errant configurations to prevent unauthorized access to the system. It will address system-defined separation of duties and include a complete discussion of the approach and strategy to maintain data integrity during all phases of system implementation and operation.

Comparable means will be employed in the interest of ensuring integrity and security of data, which include the following: field completion via a drop-down box of available choices instead of required keyed input; editing of entered data for consistency, accuracy, and completeness; limited access to the system through passwords with differing permission levels based on roles assigned to the user; and system backup procedures.

It is assumed that CNI and SPIRIT have existing security plans to address the physical security of the system, such as controlled access to facilities and computer equipment. It is further assumed that CNI and SPIRIT have a Disaster Recovery Plan in place that covers the general procedures to follow in case of disasters, which minimize disruption of operations. This Disaster Recovery Plan should address issues such as building evacuation, relocation of Tribal Agency operations to an alternate site in the event that the original location is destroyed or becomes uninhabitable, identification of emergency contacts, etc.

1. Security Planning and Administration

Security system planning and administration requires the efforts of a number of key personnel. The Security Manager writes department level policies and enforces the security policies handed down by senior management. The Security Manager should assign the primary System Administrator(s) personnel. The System Administrator is responsible for the day-to-day functions of the organization's security policy. This includes access to the WIC Management Console to perform the function of assigning users, roles, passwords, and permission levels. The System Administrator will also be responsible for performing daily backup procedures. It is the System Administrator who facilitates system security by establishing and enforcing good security planning and administration procedures. For example, a Disaster Recovery Plan may require the performance of daily backups that would be performed by the System Administrator.

In case of disaster or system failure, if the System Administrator has neglected to perform this duty then the transactions and processes for an entire day are lost. Some of the other duties assigned to the System Administrator could include set up and protection of the password file and other system-critical files, and examination of event logs.

The following paragraphs describe security planning and administration for the purpose of establishing and maintaining access control to the system.

1.1. System Access Control

The initial means of computer security provided by a security system is the control of access to that system. There are two domains with system access security in the SPIRIT WIC system: operating system domain and WIC application domain. Within both domains the following items must be addressed before a user is given access to the system:

- The users that are allowed to log into the system.
- How the system decides a user is legitimate.
- The functions that can be performed by an individual user.
- Keeping track of activities performed by individual users in the system.

In security terms, the process used by the system to determine user access to the specific domains within the system is called ***authentication and authorization***.

- ***Authentication*** refers to the user's ability to gain access to the system based on their credentials. The user provides credentials by supplying the appropriate user id and password when prompted. This is accomplished via the *Sign on* dialog. The Sign on dialog is displayed at the beginning of a *session*. A session is defined as the time span between signing on and signing off the system. During a session, access to

applications as well as features and functions within those applications is controlled through the use of Authorization.

- **Authorization** is best described as the process of checking whether or not a user has permission to access to or perform specific operations against a specific set of data. This is controlled by assigning *users* to *locations* to establish *staff member* relationships. Staff members are then assigned one or more *roles* thereby establishing the roles a user may assume while acting as a staff member of a particular location. Refer to *Application Administration – Chapter 02 – Security* for more information on establishing staff members, locations and roles.

For the SPIRIT WIC system, Tribal Agency personnel will assist in accomplishing the tasks of authentication and authorization by the following methods.

- The System Administrator will assign login identifications and passwords for each system user for the two domains in the new system.
- The System Administrator will define applications that will be available to each system user through their assigned roles in the WIC Management Console in the application domain.
- The System Administrator will assign roles, permission levels and location to users in the application domain, based on the position of the individual user and their need to access the database for each application.
- Users will use their assigned login identifications, passwords and location(s), and will be responsible for protecting them from loss or misuse.

1.1.1. Create Role Profiles

The System Administrator must define role profiles. Role profiles are more global in nature as can be used across the organization. Examples of these roles are: Nutritionist, Clerk, Administrator, Vendor Manager, etc. Each role has a comprehensive list of all *permissions* in the system. Permissions are a combination of *feature* and *access level*. Features are abstract statements that can be related to functionality in the system. An example of a feature would be ‘Participant Demographics’ (this would map to the presentation of participant demographic information within the system.) The access level associated with features can be set to one of the following; *None*, *View*, *Add* or *Full Control*. In this case, *None* would prohibit the role from viewing participant demographic information while *View* would restrict the role to a read-only view of the information, *Add* would allow the role to Add only, and *Full Control* would allow the role to View, Add, Edit, and Delete the information. Since each role has a comprehensive list of features, the access level must be set for all features in order to define the permissions for the role. By default a new role has no permissions. This is accomplished by defaulting all features to an access level of *None*. Once the roles are defined for the system, they can be added to user accounts. Note that if the permissions for a role are changed, all user accounts assigned that role will inherit the changes.

1.1.2. Create User Profiles

The System Administrator must assign login identification, location, roles and a password to each user. This is accomplished by assigning a new user account for each system user in both domains through the available user manager application on the Windows network and through the WIC Management Console.

The system Administrator will also assign the available Location(s) and Role(s) for each user profile. The permissions given to a staff member will be a combination of the highest permissions across all the roles assigned to the staff member.

This Authorization model allows for a user to be defined to one or more locations. This allows a user to be defined to a specific agency as an administrator and to a specific clinic as a Clerk (or any combination of the two). This model has value in that it allows the system administrator to define explicit access at a location level.

1.1.3. Password Development

Passwords are the primary defense that guards a system against intruders. To protect the SPIRIT WIC system and the data it contains, passwords should be well chosen and carefully protected. As this system relies on the System Administrator to generate new passwords, it will be the responsibility of the Tribal Agency to provide login identification and password information for each system user. The passwords should be complex enough to prevent duplication or guessing. They should mix uppercase and lowercase letters as well as a least one number and/or special character. The passwords should not be proper names, especially not the name of the user or one of their family members, pets, or cars. All-numeric passwords, such as a phone number or a social security number, should be avoided as well. Also, passwords should be made up of at least 6-15 characters. Lastly, different passwords should be chosen for use with various machines or applications. It may be difficult for a user to remember several passwords, but this provides security against intrusion into system data.

1.1.3.1.1. Password Format

A password format makes it unnecessary for the password to be gibberish. The average user will be more tempted to write down a password of gibberish and thereby defeat the purpose of a carefully selected password. Some possible password formats follow.

- Combination of several short words with numbers or special characters, like "I;did3it".
- Use of an acronym built from a phrase that is easy to remember but difficult to recognize. For example, the acronym for the recognizable phrase "When in the course of human events" is "Witcohe" and might be guessed. It is better to pick a phrase that

is not as recognizable. For example, the acronym for “Oh no, I forgot to do it” is “Oniftdi”.

- Include a number or special character for increased security. For example “Onif;tdi” or “On5iftdi”.
- Pick nonsense words that are still pronounceable; for example “8Bektag” or “shmoaz12”.

1.1.3.1.2. Protecting Passwords

Most systems protect passwords in two ways. First, they make passwords difficult to guess and login controls hard to crack, and second they protect the file in which passwords are stored. The following list will explain how the System Administrator can aid the system in protection of passwords.

- Limit the number of attempts that can be used to gain entry into the system. After the set number of unsuccessful attempts the system locks out the potential user, preventing them from accessing the data. The user then has to start the application again and reenter their login and password. In this system the number of attempts is 3.
- Require the users to change their passwords at specified intervals, and deny access to the system for users with an expired password. This security tactic can also be used to keep former employees from gaining access to the system when they are no longer employed by the State. In this system, the user is required to change their password every 90 days.
- Determine a minimum character length for passwords. In this system the minimum password length is 6 to 15 characters.
- Include a multi-password mechanism that requires the user to log into different domains before starting the new application. This multi-password mechanism further limits access to system applications by non-authorized personnel. In this system, the users will be required to login to their desktop/network domain before gaining access to the WIC domain.
- Require case-sensitive passwords. In this system the password is case-sensitive.

1.2. Separation of Duties

The principle of Separation of Duties states that no single individual has total control of all system security mechanisms. For example, the System Administrator has total control of daily operations and security functions of the system. This includes assigning new user accounts, terminating user accounts, deleting old users from the system, creating additional space in the database, etc.

However, when this individual takes vacation and sick days another person must accomplish these daily tasks. Instead the Alternate System Administrator can function as the Security Manager, which allows the Primary System Administrator to perform the daily functions of the system. This ensures that the Separation of Duties principle is followed and that one individual does not have total control of the system security functions.

1.3. Performing Backups

The performance of daily system database backup is one of the most important functions entrusted to the System Administrator. These backups are vital in case of system crash or invasion of the system by a virus. They should be performed as part of the daily processing to ensure that no data loss occurs in the event of a system malfunction.

The database backup will be performed and stored to tape, using a process developed by CNI specifically for SPIRIT. Once the backup is complete the tape should be removed from the tape drive and stored in a safe location for emergency recoveries, and a new tape inserted into the drive. It is recommended that the backup tapes be rotated on different days, so that the same tape is not always used on the same day of the week. This will increase the life of the tape and ensure that all data are saved each time the backup is performed.

Once a laptop is checked out, the data on the laptop is no longer on-line. This data will not be included in the system backups that occur on the primary database server. Covansys recommends that daily backups of the data be performed on all satellite servers/laptops that are checked out. It is recommended that the personnel utilizing this equipment be trained on proper backup procedures for the satellite server databases.

2. System and Data Integrity

This section addresses the establishment and maintenance of system and data integrity. Broadly defined, system integrity involves the continued correct functioning of a system. In the same broad terms, data integrity involves the maintenance of both system and participant data in its most recently updated form.

2.1. System Integrity

Compromise in system integrity includes events such as system failure due to missing or mismatched modules and other operational synchronization problems. As a result, the application fails to perform as designed. This can result in data loss, work loss, and/or the inability to provide services.

During development, the new system application software is kept in a software library application called Source Mountain. Only authorized development staff has access to this software. As software changes are made and released into the field, a version control number is assigned to the software for tracking purposes.

System integrity in the field will be maintained principally through an automatic software version control process. This process utilizes a version tracking number to assure all of the software components are part of the same software release. The process compares the version of the software and reference tables loaded on the application server for the latest version. If it is not correct, the process automatically updates the software components from the software Repository. This assures that software updates are quickly and consistently applied, thereby lessening the risk that outdated versions of the applications are in use.

Each time a new version of the software is released, Covansys will provide SPIRIT with a document advising them of important software release information. Included in this software release document are the following: the latest version identification number and label; the date of distribution for the new software version; and any problems or issues that could be encountered in the distribution of the software version.

2.2. Data Integrity

Data integrity can be compromised if the data is unusable due to damage, loss, inconsistency, or inaccuracy. For instance, if data elements become corrupted, lost, or fail to match other related pieces of data then the integrity of the data is compromised. In the development of the SPIRIT WIC system, there are three phases in which data integrity might be compromised: conversion, implementation, and operations.

2.2.1. Conversion

Significant planning and preparation are necessary to ensure the preservation of data integrity when it is converted from the legacy system. In

many cases, a direct one to one correlation exists between data in the legacy system and what is required in the new system. In some cases, no comparable data may be available in the legacy system to populate the new system fields. In these cases, appropriate default values must be assigned.

The data conversion process itself will be as automated as possible to minimize the risk of human error. There will be controls and checkpoints included throughout the process to insure that all appropriate data are converted accurately.

The various steps and controls to be used during conversion of the legacy data into the new system are described in detail in the Conversion Plan, which is independent of this document. This plan is subject to SPIRIT review and approval, and will help to ensure maximum data integrity during the conversion process.

2.2.2. Implementation

Once converted, the data will be loaded onto the database server for each Tribal Agency at the CNI office and normal system operations can begin. Each Tribal Agency will establish a schedule that includes the final day that information may be processed in the legacy system, which assures that the most recent data, is available for conversion. Also, all Tribal Agency staff must be trained on the new system so that each staff member fully understands how to use the system. Finally, a detailed process of equipment configuration, software installation, and converted database loading at the CNI office will be performed. For additional information, refer to the *Implementation Plan*.

2.3. Operations

Once the data is converted and implemented, data integrity will be maintained through normal operational controls at the CNI office location. Responsibility for data integrity will be the responsibility of the CNI IT personnel from this point forward.

2.3.1. Local Clinics

Data integrity at the WIC clinics will be maintained at both the record and field levels within the centralized database. As the majority of the data input will occur at these sites, proper training and system design are imperatives that will maximize data integrity.

All staff scheduled to use the system will receive intensive training. This training will lessen the risk for erroneous data entry or accidental misuse that might compromise data integrity. For more information, refer to the *Training Plan*.

The SPIRIT WIC system has been designed for strict control of data input where possible to help ensure accuracy. The system makes extensive use of

drop down selection lists for fields that have finite choices. This allows the user to select from a list of valid field values, and eliminates the possibility of key errors and/or invalid data in those fields. Additionally, fields that accept highly variable entry, where drop down selection lists are not available, are equipped with extensive edits and cross-edits to insure that only valid data is entered. Sequential field values, such as next available ID number, are automatically determined by the system based on other available data to eliminate the risk of human error.

3. System Security

This section addresses the establishment and maintenance of software and data security. Broadly defined, system security involves measures taken to protect the SPIRIT WIC system from a loss of data that might compromise system operation, performance or confidentiality. In the development of the system, there are three phases in which system security might be compromised: conversion, implementation, and operations.

3.1. Conversion

Conversion of legacy system data into the SPIRIT WIC system will occur at the CNI facilities in Oklahoma. Entry into the computer rooms that house the conversion equipment are continually locked and controlled by electronic access cards requiring a higher permission level.

In addition to limiting access to facilities and equipment, access to data on the conversion equipment is restricted through a rigorous system of password and user ID protections. Only individuals who require data access to complete the conversion process have appropriate system security clearance.

3.2. System Security

System security tests for the WIC Applications will be conducted throughout unit and regression testing by the development and quality assurance teams at Covansys. CNI will conduct Network and Internet security testing at the CNI offices. All known issues with security will be resolved prior to UAT. If additional security issues are found during UAT, either Covansys or CNI will resolve the issues prior to Pilot and Implementation. CNI will be responsible for resolving security issues that arise after implementation.

3.3. Internet Security

CNI is responsible for installing Norton Antivirus Corporate Edition or similar antivirus software on all computers. CNI will be responsible for configuring the antivirus software. The antivirus software should be configured so that virus definition updates are run automatically without user interaction. All users should be trained on the following

- Verifying the Virus Definition File is up to date
- Performing Live Updates
- Accessing/Opening the antivirus software.
- Running a full system virus scan.
- Running a virus scan on a single file
- Risks associated with opening email attachments from unknown persons.

CNI will be responsible for installing and configuring Firewall protection.

3.4. Implementation

Once converted, the data will be loaded onto the database server at the CNI office and normal system operations can begin. From this point the data is protected by normal system and application security procedures.

It should be noted that all equipment that is part of the SPIRIT WIC system will be 'wiped clean' by the implementation teams at the time of equipment setup. This removes any residual backdoors into the computer system that may have existed prior to the implementation. This also removes any unauthorized software that might conflict with the new applications.

3.5. Operations

Once converted and implemented, system security is maintained through normal operational controls at the various locations where operations occur.

3.5.1. System Security

System security is comprised of three layers of access control. The first layer consists of the operating system identification and authentication procedures of each computer. A user will be required to logon through the operating system when starting up the computer.

Once the user has logged on to the operating system, the second layer of access control consists of the identification and authorization through the WIC Management Console to gain access to the WIC applications.

The third layer of access control exists within the SPIRIT WIC applications. When starting an application, the system will check the permission levels assigned to the user. If the user attempts to access an application where they do not have permissions, a warning message is displayed, indicating they do not have permission and the application will terminate.

System security can be maintained only if all personnel practice the prescribed security measures. These include basic measures such as avoiding passwords that could be easily guessed, sharing passwords, and failing to log off when a workstation is left unattended. By carefully observing the security guidelines set out in this document, SPIRIT can ensure maintenance of system and data integrity.

4. Recommendations For Non-Computer Related Tasks

This section addresses the recommendations by Covansys for non-computer related tasks. It is presumed by Covansys that the SPIRIT WIC Program will have policies and procedures to account for these type of situations. Some of the policies and procedures may already exist.

4.1. Check Stock

It is understood that SPIRIT will use blank check stock. In the case where pre-printed check stock is used, it is recommended the handling of check stock be assigned to one staff member and a back-up staff member. If the printers being ordered for the WIC printing of food instruments have locks and keys for the check trays those trays will be locked during business hours and the key will be in possession of a designated staff member. At the end of the day all unused check stock will be removed from the printer trays and secured in a defined location within the WIC Clinic. All other unused check stock will also be secured in a defined location within the WIC Clinic.

A designated staff member will be responsible for the Queue Manager application and the check printer for which produced the participant food instruments. A designated staff member will be responsible for signature of receipt for the boxes of checks.

4.2. Compliance Buy Checks

It is understood that SPIRIT will use blank check stock. In the case where pre-printed check stock is used, Compliance buy checks will be created at the State Office by designated Vendor Management staff. These checks will be used for monitoring visits to various vendors. The record of the visit will be entered into the Vendor Management application. A recommendation is for SPIRIT to have a secondary log of all compliance buy checks for when the check was created, by whom, and how it was used.

All check stock should be secured in a designated location.

4.3. Printers

It is recommended for printers at the clinics to be located in a non-customer public area. This will assist in the privacy of customers. Therefore, curbing the possibility of documents being picked up by visitors within the clinic.

4.4. Monitoring positioning to customer view

It is recommended for PC monitors to be positioned that present security to staff and customers. This will assist in the privacy of customers.