Community Shelter Board

Columbus ServicePoint (CSP)

Policies and Procedures

Last Revised: 04/2019

TABLE OF CONTENTS

1. Introduction

1.1 Community Shelter Board

VISION

Everyone has a place to call home.

MISSION

Community Shelter Board leads a coordinated, community effort to make sure everyone has a place to call home. CSB is the collective impact organization driving strategy, accountability, collaboration, and resources to achieve the best outcomes for people facing homelessness in Columbus and Franklin County.

1.2 Project Summary

Columbus ServicePoint (CSP) is used to collect, monitor, and evaluate homeless and housing services in Columbus and Franklin County. Currently, over 260 users in 16 agencies are using CSP to collect data for over 90 homeless and housing related programs throughout Franklin County. The CSP project is supported by CSB through a Data and Evaluation Department staffed by a full time CSB Database Administrator, Data and Evaluation Manager, Operations Administrator and Operations Director.

HUD requires each local CoC to have an HMIS that complies with the HUD standards, is used by all HUD funded entities in the continuum and is able to produce aggregate reporting at system and community level. Prior to 2008, CSB's HMIS did not fully comply with these standards, which led to the need to upgrade the system.

To comply with the above requirements, a community-wide HMIS Selection Committee was convened and supported by CSB to implement a plan to upgrade the existing HMIS.

The HMIS Upgrade RFP was issued in January of 2007. The HMIS Selection Committee deemed that three vendors warranted further consideration. A thorough due diligence process was performed for each of the three vendors to determine the best system. The Committee recommended on September 11, 2007 to start contract negotiations with Bowman Systems (now Wellsky) as the vendor for the upgraded HMIS. The recommendation was presented and adopted by the CoC Steering Committee on October 9, 2007. Implementation of the new system was started in November 2007. The eight-month implementation process was coordinated through a community-wide implementation planning team with representation from all agencies using HMIS. The implementation due date and "go live" date was July 14, 2008.

1.3 Governing Principles

The goal of CSP is to support the delivery of homeless and housing services in Columbus and Franklin County. CSP is:

- a benefit to individual clients through enhanced service delivery
- a tool for the provider agencies in managing programs and services
- a guide for CSB and its funders regarding community resource needs and service delivery

While accomplishing these goals, CSB recognizes the primacy of client needs in the design and management of CSP. These needs include both the need continually to improve the quality of homeless and housing services in Columbus and Franklin County, and the need vigilantly to maintain client confidentiality, treating the personal data of our most vulnerable populations with respect and care. As the guardians entrusted with this personal data, we have both a moral and a legal obligation to ensure that this data is being collected, accessed and used appropriately. The needs of the people we serve are the driving forces behind CSP.

With this in mind, CSP will also be:

- a **confidential and secure environment** protecting the collection and use of client data

1.4 Terminology

Definitions of some of the terms used in this manual are as follows:

Authentication: The process of identifying a user in order to grant access to a system or resource. Usually based on a username and password.

CSP: The specific HMIS utilized in Columbus, Ohio.
A software package developed by Wellsky which tracks data about people in housing crisis in order to determine individual needs and provide aggregate data for reporting and planning. This software is web-based and uses a standard web browser to access the database.

Contributing HMIS Organization (CHO): Any agency, organization or group who has signed a CSP Agency Agreement with CSB and is allowed access and contributes data to the CSP database. These agencies connect independently to the database via an internet web browser.

Continuum of Care Project: Project receiving funding from the US Department of Housing and Urban Development through the competitive Continuum of Care application process.

CSB: Community Shelter Board. CSB is an intermediary funding and planning organization in Columbus, Ohio, with the goal of eliminating homelessness in Columbus and Franklin County.

CSB Database Administrator: The job title of the person at CSB who is the System Administrator for CSP.

Database: An electronic system for organizing data so it can easily be searched and retrieved. Usually organized by fields and records.

Encryption: Translation of data from plain text to a complex code. Only those with the ability to unencrypt the encrypted data can read the data. Provides security.

Firewall: A method of controlling access to a private network, to provide security of data. Firewalls can use software, hardware, or a combination of both to control access.

Partner Agency: Agencies receiving funding from Community Shelter Board.

Server: A computer on a network that manages resources for use by other computers in the network. For example, a file server stores files that other computers (with appropriate permissions) can access. One file server can "serve" many files to many client computers. A database server stores a data file and performs database queries for client computers.

Agency Administrator: The person responsible for system administration at the agency level. Responsible for adding and deleting users, basic trouble-shooting, quality assurance of data and organizational contact with the CSB Database Administrator.

System Administrator: The person with the highest level of user access in CSP. This user has full access to all user and administrative functions. The name of the level of access is "System Administrator II."

User: An individual who uses a particular software package; in this case, the CSP software.

User License: An agreement with a software company that allows an individual to use the product. In the case of CSP, user licenses are agreements between CSB and Wellsky that govern individual connections to CSP.

Wellsky: Formerly known as Bowman/Mediware Information Systems. The company who developed the software used for CSP.

1.5 Ownership

CSP, and any and all data stored in CSP, is the property of the Community Shelter Board. CSB has final control over the creation, maintenance and security of CSP. In order to ensure the integrity and security of sensitive client confidential information and other data maintained in the database, CSB will require all CHOs to sign an agreement ("Agreement") prior to being given access to CSP. The Agreement includes terms regarding the confidentiality of client information, duration of access, an acknowledgement of receipt of the Policies and Procedures Manual, and an agreement to abide by policies and procedures related to CSP, including all security provisions contained therein.

Violations of the Agreement, including without limitation the failure to comply with the policies and procedures related to CSP, may subject the Contributing HMIS Organization (CHO) to discipline and termination of access to CSP and/or to termination of other CSB contracts.

2. Implementation Overview

2.1 Relationship to CHOs

Contributing HMIS Organizations (CHOs) are those agencies allowed by CSB to connect to CSP for the purposes of data entry, data editing and data reporting. These agencies are CSB Partner Agencies and Other Agencies. Partner Agencies are agencies receiving funding directly and/or pass-through from Community Shelter Board. Other Agencies choose to participate in the CSP though they do not receive funding from Community Shelter Board.

Relationships between CSB and CHOs are governed by any standing agency-specific agreements already in place (such as the Program and Master Provider Agreements), the CSP Agency Agreement, and the contents of the Policies and Procedures Manual. All CHOs, regardless of type, are required to abide by the policies and procedures outlined in this manual.

2.2 Relationship to Wellsky

CSB contracts with Wellsky on an annual basis. Through this contract, Wellsky provides software maintenance, application support, and database maintenance and hosting. CSB has purchased software and user licenses, for an annual fee, to be used to access CSP. CSB is responsible for maintaining the CSP contract with Wellsky, and the CSB Database Administrator is the designated contact to Wellsky. The CSB Database Administrator is responsible for providing the main conduit for communications between CHOs and Wellsky in order to provide coherent and timely information exchange.

While most communications with Wellsky related to CSP will be channeled through the CSB Database Administrator, CHOs may choose to contract independently with Wellsky to acquire further database customization or other services not related to CSP. In such cases, the individual agency is solely responsible for negotiation of, and payment for, these services, as well as all communication with Wellsky regarding these matters.

2.3 Central Server

CSP is hosted on Wellsky's servers, located in a larger office complex with 24-hour security. The Wellsky network is protected by strong firewalls, and all traffic is logged and monitored by System Administrators. The database server utilizes RAID disk mirroring to protect data in the event of hard drive failure, and all data is backed up on a nightly basis and secured in an off-site, fire proof storage facility.

CSP grants access only to authorized users by utilizing username and password authentication. CSP supports commercial-grade, TLS1.0/1.1/1.2 browser encryption. CSP also includes multiple security levels to control the amount of access a valid user can have.

2.4 Security Infrastructure

CSB, by paying a monthly fee, is taking advantage of Wellsky's maintenance and hosting services for CSP. Wellsky employs a full time staff of experts dedicated to keeping their clients up, running and secure, using the latest technology. This technology includes physical security, Cisco firewalls, authentication through browser certificates, Windows secure server technology, and encryption of usernames, passwords, and all data passing to and from the database. It is the job of the CSB Database Administrator to maintain a point of contact between Wellsky and CSB and keep track of security issues at the central database.

This arrangement provides protection against:

Physical Attack: The Wellsky servers are located in a physically secure building, where security guards are employed to monitor security from 7:00 a.m. to 7:00 p.m. Monday through Friday, and from 8:00 a.m. to 4:00 p.m. on Saturdays. During off-hours, a card key is required to enter the building. Within the building, the Wellsky offices are also locked with a separate key structure.

Network Attack: Wellsky uses Cisco firewalls to prevent unauthorized remote access to the database server. A firewall is a software application which blocks all incoming electronic traffic except traffic that is explicitly permitted. Permissions are configured manually by network administrators. This combination of firewalls and virus protection software will detect and prevent most viruses, Trojan horses, worms, malicious mobile codes or email bombs from damaging our database.

Denial of Service: The combination of firewalls and routine monitoring of network traffic by skilled professionals (in this case, Wellsky network administrators) will detect and prevent an attacker from flooding our server to the point of failure.

Exploitation of Operating System Vulnerabilities: As a part of the maintenance contract, network administrators at Wellsky are responsible for updating the server with the latest software patches and fixes of known operating system weaknesses. Keeping abreast of software patches and reports of new vulnerabilities is the best way to avoid falling prey to these attacks.

Exploitation of Software Vulnerabilities: Because we rely on the same company who created the CSP software to host our system, we can be sure that any security holes discovered in the software will be addressed by technicians with access to timely and accurate information about the core program. We do not need to rely on second or third-hand software alerts, or the installation of patches and upgrades by network administrators unfamiliar with the product. This is a great advantage in combating application-specific security issues.

User Falsification: Using a public-key infrastructure and signed digital certificates provides a safe and reliable method of authenticating users. These methods, while they do employ traditional user names and passwords at their base, encrypt data and provide a software-enabled check and counter-check methodology that make stealing identities or masquerading as an authorized user virtually impossible. In addition, these methods produce one-time use session keys that foil a replay attack, as user credentials will never be signed and encrypted in precisely the same way twice.

Data Traps: Wellsky supports TLS encryption of all data passing from agency to server, or server to agency. Encryption is the translation of data from a readable "clear text" to an encoded hash using complex mathematical algorithms. TLS, short for Transport Layer Security, is a data transport protocol which encrypts data using a public-key infrastructure. When data is encrypted, even if information packets could be captured or recorded as they travel across the Internet, they could not be decoded and read.

Server Falsification: The public-key infrastructure provides not only authentication of the agency, but also authentication of the web site, and hence, authentication of the hosting server. Authentication is provided through digital certificates and is an integral part of the login process. Mutual authentication prevents a rogue web site from masquerading as our secure web site and drawing sensitive data.

Social Engineering: These are attacks in which a social situation (for example, a customer service call from a third-party company) is manipulated so that an unauthorized user gains access to protected information, such as a client data, or user names and passwords. The biggest deterrent to social engineering is clear policies and procedures. It is much harder for users to be manipulated into providing confidential information if they have clear and thoughtful rules to follow when providing such information. CSB provides clear and thoughtful policies and procedures around issues of CSP data confidentiality, and confidentiality of user names and passwords. These procedures are designed to speed problem resolution and minimize the chance of a user being manipulated into divulging confidential data through confusion or a sincere desire to help someone in need.

Misuse of Privileges: CSP provides several levels of user access to the database. Each level has access to a particular subset of information, and particular abilities to manipulate information. CSB provides clear "job descriptions" for each level of access, to ensure that each user is assigned an appropriate level of access. CSB also provides clear protocol and procedures for handling data needs and requests that fall outside of a particular user's job description. Finally, CSB provides clear procedures for handling changes in access levels and users, as well as for password recovery and other access issues. These procedures are designed to clarify and streamline the daily work of legitimate users, and minimize the chance of legitimate users misusing privileges even towards legitimate ends.

Local Physical Attack: Agency computers are more physically vulnerable than our central server. As no CSP data is stored on the local computer, however, the physical vulnerability of these computers does not constitute a significant threat to client confidentiality regarding this data. However, any user access data, such as a password, that is stored on a computer or in a written file, does constitute a risk to client confidentiality. CSP policies and procedures include provisions for the appropriate handling of client access data.

3. Roles and Responsibilities

3.1 Project Organization

3.1.1 Project Management

Policy: CSB is responsible for organization and management of CSP.

Explanation: As the coordinating body for CSP, Community Shelter Board is responsible for all system-wide policies, procedures, communication and coordination. CSB is the primary contact with Wellsky, and with its help, implements all necessary system-wide changes and updates.

Procedure: CSB seeks to provide a uniform CSP which yields the most consistent data for client management, agency reporting, and service planning. The primary position at CSB for CSP management is the CSB Database Administrator. All system-wide questions and issues should be directed to the CSB Database Administrator. The Database Administrator reports to the CSB Operations Director. The Operations Director designates a Back-up Database Administrator. CSB's Executive Director, as head of the Community Shelter Board, is ultimately responsible for all final decisions regarding planning and implementation of CSP.

3.1.2 Agency Administrator

Policy: Each CHO designates an Agency Administrator. The Agency Administrator must have an email address.

Explanation: The Agency Administrator is the primary CSP contact at the agency. This person is responsible for:

- Providing a single point of communication between the CHO's end users and the CSB Database Administrator around CSP issues
- Ensuring the stability of the agency connection to the Internet and CSP, either directly or in communication with other technical professionals
- Training agency end-users
- Providing support for the generation of agency reports
- Managing agency user licenses
- Monitoring compliance with standards of client confidentiality and data collection, entry, and retrieval
- Participating in Agency Administrators training and regular meetings
- Participating as the advisors and consultants to the CSB Database Administrator

Designating one primary CSP contact and power-user at each agency increases the effectiveness of communication both between and within agencies.

Procedure: Each CHO designates its Agency Administrator and sends that person's name and contact information to the CSB Database Administrator. Changes to that information should be promptly reported to the CSB Database Administrator. Each CHO designates a back-up Agency Administrator and sends the person's information to CSB Database Administrator.

3.1.3 User Access Levels

Policy: All CSP Users have an appropriate level of access to CSP data.

Explanation: CSP allows multiple levels of user access to data contained in the database. Access is assigned when new users are added to the system and can be altered as needs change. For security purposes, appropriate access levels should be assigned to all users.

Procedure: The Agency Administrator, in consultation with the CSB Database Administrator, assigns appropriate user levels when adding new users. In the interest of client data security, the Agency Administrator will always attempt to assign the most restrictive access which allows efficient job performance.

3.1.4 CSB Communication with CHOs

Policy: The CSB Database Administrator is responsible for relevant and timely communication with each agency regarding CSP.

Explanation: The CSB Database Administrator communicates system-wide changes and other relevant information to agencies as needed. The CSB Database Administrator also maintains a high level of availability to CHOs. While specific problem resolution may take longer, the CSB Database Administrator strives to respond to CHO questions and issues within one business day of receipt.

Procedure: General communications from the CSB Database Administrator are directed towards the agency Agency Administrator, most of the time through email communication. Specific communications will be addressed to the person or people involved. The CSB Database Administrator is available via email, phone, and mail. The CSB website is used to distribute CSP information. Agency Administrators are responsible for ensuring all their agency users are informed of appropriate CSP related communications. Agency Administrators are also responsible for distributing that information to any additional people at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers, and data entry specialists.

3.1.5 CHO Communications with CSB

Policy: CHOs are responsible for communicating needs and questions regarding CSP directly to the CSB Database Administrator. For CSP IT requests, the CHO uses Spiceworks to submit support tickets.

Explanation: CHOs communicate needs and questions directly to the CSB Database Administrator. For IT support tickets, the CHO uses Spiceworks to communicate issues with CSB. The Data and Evaluation team reviews the Spiceworks tickets and provides an initial response to the CHO within 24 hours.

Procedure: Users at CHOs communicate needs, issues and questions to their Agency Administrator. If the Agency Administrator is unable to resolve the issue, the Agency Administrator contacts the CSB Database Administrator via email, phone, mail, or Spiceworks support ticket. The goal of the CSB Database Administrator is to respond to CHO needs within one business day of the first contact.

3.1.6 System Availability

Policy: CSB and Wellsky provide a highly available database server and inform users in advance of any planned interruption in service.

Explanation: It is the intent of CSB and Wellsky that the CSP database server will be available 24 hours a day, 7 days a week, 52 weeks a year to incoming connections. However, no computer system achieves 100% uptime. In the event of planned server downtime, the CSB Database Administrator informs agencies as much in advance as possible in order to allow CHOs to plan their access patterns accordingly.

Procedure: In the event that the database server is or will be unavailable due to disaster or routine maintenance, Wellsky contacts the CSB Database Administrator. The CSB Database Administrator contacts Agency Administrators and informs them of the cause and duration of the interruption in service. The CSB Database Administrator logs all downtime for purposes of system evaluation.

3.1.7 Ethical Data Use

Policy: Data contained in CSP is used to support the delivery of homeless and housing services in Columbus and Franklin County. Each CSP User affirms the principles of ethical data use and client confidentiality contained in the CSP Policies and Procedures Manual and the CSP User Agreement.

Explanation: CSB recognizes that the specific purpose for which the CSP was created limits the uses of the data it contains to those which conform to this initial purpose. The data collected in CSP is the personal information of people in the Columbus and Franklin County community who are experiencing a housing crisis. It is the responsibility of the guardians of that data to ensure that it is only used to the ends to which it was collected.

Procedure: All CSP users sign a CSP User Agreement before being given access to CSP. Any individual or CHO misusing, or attempting to misuse, CSP data will be denied access to the database, and his/her/its relationship with CSB will be terminated.

3.1.8 CHO Grievances

Policy: CHOs contact the CSB Database Administrator to resolve CSP problems.

Explanation: CSB is responsible for the operation of CSP. Any problems with the operation or policies of CSP are to be discussed with the Community Shelter Board. CSB has final decision-making authority over all aspects of CSP.

Procedure: CHOs bring CSP problems to the attention of the CSB Database Administrator. If these problems cannot be resolved by the CSB Database Administrator, the CSB Database Administrator will take them to the CSB Operations Director, and finally to the CSB Executive Director. CSB's Executive Director shall have the final say in all matters regarding CSP.

3.1.9 Client Grievance

Policy: Clients contact the CHO with which they have a grievance for resolution of CSP problems. CHOs report all CSP-related client grievances to the Community Shelter Board.

Explanation: Each agency is responsible for answering questions and complaints from their own clients regarding CSP. CSB is responsible for the overall use of CSP, and will respond if users or agencies fail to follow the terms of the CSP Agreements, breach client confidentiality, or misuse client data. Agencies are obligated to report all CSP-related client problems and complaints to the Community Shelter Board, which will determine the need for further action.

Procedure: Clients bring CSP complaints directly to the agency with which they have a grievance. Agencies provide a copy of the CSP Policies and Procedures Manual upon request, and respond to client issues. Agencies send copies of all client grievance forms recording CSP-related client problems and complaints to the CSB Database Administrator. The CSB Database Administrator records all grievances and reports these complaints to the CSB Operations Director, who will take any necessary action. The CSB Database Administrator keeps a log of all complaints and concerns, and responds to individual complaints and patterns of concern with appropriate actions. These actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and agencies if users or agencies are found to have violated standards set forth in Agreements or the Policies and Procedures Manual.

3.1.10 CHO Hardware/Software Requirements

Policy: CHOs provide their own computer and method of connecting to Internet, and thus to CSP.

Explanation: Because CSP is a web-enabled software, all that is required to use the database is a computer, a valid username and password, and the ability to connect to the Internet by broadband or other high-speed connection. There is no unusual hardware or additional CSP-related software or software installation required. Wellsky guidelines are:

WORKSTATIONS

ServicePoint 5 relies on the client machine more than previous versions. Therefore, faster machines will have better results, where in the past most of the performance was related to the server and connection speed. Fast internet connection and browser speed are still important.

MEMORY
4 Gig recommended, (2 Gig minimum)

MONITOR
Screen Display - 1024 by 768 (XGA) or higher (1280x768 strongly advised)

PROCESSOR
Avoid using single-core CPUs

INTERNET CONNECTION
Broadband or other high-speed option

BROWSER
Mozilla Firefox is recommended; Internet Explorer, Microsoft Edge and Google Chrome are acceptable.

Procedure: It is the responsibility of the CHO to provide a computer and connection to the Internet. If desired by the CHO, the CSB Database Administrator will provide advice as to the type of computer and connection.

3.1.11 CHO Technical Support Requirements

Policy: CHOs provide their own technical support for all hardware and software employed to connect to CSP.

Explanation: The equipment used to connect to CSP is the responsibility of the CHO.

Procedure: Agencies provide internal technical support for the hardware, software and Internet connections necessary to connect to CSP according to their own organizational needs.

3.1.12 CSP Documentation Updates (Policies & Procedures, User's Manual, QA Standards & Data Dictionary, and CSP related forms)

Policy: CSB provides a CSP Policies & Procedures Manual, QA Standards & Data Dictionary, and relevant forms and user guides for all CSP Agency Administrators. These documents are kept up to date and in compliance with all HUD policies and requirements.

Explanation:
The purpose of the CSP policies and procedures is to provide Agency Administrators with guidance in maintaining compliance with HUD and Continuum of Care requirements and standards. They include information about how the software product is to be managed from an Agency Administrator perspective and the roles and responsibilities of an Agency Administrator and their CHO. CSB provides an electronic copy of the Policies and Procedures Manual containing procedures that are held in common for all CHOs.

A CSP Agency Administrator manual provides information about how the software product is used in our community, contains procedures that are held in common for all CHOs, and includes common CSP related forms. The manual also provides specific technical instruction about how to use CSP. The QA Standards & Data Dictionary provides detailed information on the quality assurance standards and the data requirements for all programs and CHOs. CSB provides an electronic copy of the QA Standards & Data Dictionary for all CHOs.

Procedure: The CSB Database Administrator updates the Policies & Procedures, QA Standards & Data Dictionary and commons CSP related forms and user guides annually, by the beginning of each new fiscal year. The CSP documents are reviewed and kept up to date and in compliance with all HUD policies and requirements. In the event HUD issues interim changes to the requirements, affected policies and procedures and related documentation are reviewed and updated at that time as well. The updates are reviewed and approved by the CSB Operations Director. The updates are communicated and discussed with the CSP Agency Administrators during the quarterly CSP Administrator meetings. If HUD requirements necessitate immediate implementation of changes, this will be communicated to all Agency Administrators electronically, as soon as available. Regular CSP trainings include an overview of these documents and their role. These documents will be available for download at www.csb.org.

3.2 Security

3.2.1 User Access

Policy: Agency Administrators provide unique usernames and initial passwords to each agency user. Usernames are unique for each user and are comprised of the initial of the user's first name and the user's full last name, all lower case. Usernames and passwords may not be exchanged or shared with other users. The CSB Database Administrator has access to the list of usernames.

Explanation: Unique usernames and passwords are the most basic building block of data security. Not only is each username assigned a specific access level, but in order to provide to clients an accurate record of who has altered his or her record, when it was altered, and what the changes were, it is necessary to log a username with every change. Exchanging usernames seriously compromises security and accountability to clients.

Procedure: Agency Administrators provide unique usernames comprised of the user's first initial and full last name, all lower case, and initial passwords to each user upon completion of training and signing of a confidentiality agreement and receipt of the Policies and Procedures Manual. The sharing of usernames is considered a breach of the Agreement.

3.2.2 User Changes

Policy: The CHO Agency Administrator makes any necessary changes to the role of CHO users.

Explanation: The Agency Administrator has the ability to add/delete user accounts and re-distribute user licenses to accommodate agency needs.

Procedure: The Agency Administrator makes any necessary changes to the list of agency users. Changes in Agency Administrators and backup Agency Administrators must be reported to the CSB Database Administrator.

3.2.3 Passwords

Policy: Users have access to the CSP via a username and password. Passwords reset every 45 days. Passwords must consist of at least 8 characters and include at least two digits. Users keep passwords confidential.

Explanation: Users have access to the CSB CSP via a username and password. This method of access is unique to each user and confidential. Users are responsible for keeping their passwords confidential. For security reasons, passwords are automatically reset every 45 days.

Procedure: The CHO Agency Administrator issues a username and password to each new user who has completed training directed by the CHO. Every 45 days, passwords are reset automatically. On the 45th day, when the user logs in, the system requires the user to create a new password and enter it twice before accessing the database.

3.2.4 Password Recovery

Policy: The CHO Agency Administrator resets a user's password in the event the password is forgotten. CSB's Database Administrator resets an Agency Administrator's password in the event the password is forgotten.

Explanation: In the event of a forgotten password, the CHO Agency Administrator resets that password, deleting the old password and allowing the user to connect using a new temporary password.

Procedure: In the event of a forgotten password, the user whose password is forgotten contacts the Agency Administrator. The Agency Administrator resets the user password, and issues a temporary password to allow the user to login and choose a new password. The new password is valid from that time forward, until the next password expiration.

3.2.5 Extracted Data

Policy: CSP users maintain the security of any client data extracted from the database and stored locally, including all data used in custom reporting. CSP users do not electronically transmit any unencrypted client data across a public network. CSB may initiate encrypted electronic communication via secure email.

Explanation: The custom report-writer function of CSP and ART allows client data to be downloaded to an encrypted file on the local computer. Once that file is unencrypted by the user, confidential client data is left vulnerable on the local computer, unless additional measures are taken. Such measures might include restricting access to the file by adding a password. For security reasons, unencrypted data may not be sent over a network that is open to the public. For example, while unencrypted data might be stored on a server and accessed by a client computer within the private local area network, the same unencrypted data may not be sent via email to a client computer not within the same local area network. CSB may initiate encrypted electronic communication via NeoCeritified secure email. Replies to these emails must be done through the NeoCertified secure reply interface, by clicking the link within the email, to maintain confidentiality of any sensitive information. CSP users should apply the same standards of security to local files containing client data as to the CSP database itself.

Procedure: Data extracted from the database and stored locally is stored in a secure location and is not transmitted outside of the private local area network unless it is properly protected. Security questions are addressed with the CSB Database Administrator.

3.2.6 Data Access Location

Policy: Users ensure the confidentiality of client data, following all security policies in the CSP Policies and Procedures Manual and adhering to the standards of ethical data use, regardless of the location of the connecting computer.

Explanation: Because CSP is web-enabled software, users could conceivably connect to the database from locations other than the agency itself, using computers other than agency-owned computers. If such a connection is made, the highest levels of security must be applied, and client confidentiality must still be maintained. For situations where this type of access may be needed regularly, please see the Remote Access Policy 3.2.9.

Procedure: All Policies and Procedures and security standards are enforced regardless of the location of the connecting computer.

3.2.7 Hardware & Software Security Measures

Policy: The Agency Administrator ensures all hardware and software used to access and/or store CSP data is in a secure location where access is restricted to authorized staff. The Agency Administrator ensures all computers used to access and/or store CSP data employ software security and access restriction measures.

Explanation: Because CSP enables authorized users to download raw client-level data via the Custom ReportWriter or ART to their hard drive or other electronic media, access to such computers and/or disks must be restricted to authorized personnel only.

Procedure: The Agency Administrator ensures that any computers used to access CSP and any disks used to store custom report information are located in a secure area where access is available to authorized personnel only. The Agency Administrator ensures that these same computers and disks utilize the following security measures listed below.

Computers:

- Locking screen savers
- Virus protection with auto update
- Individual network firewalls

Storage disks:

- Encryption (Examples of software which can be used for file encryption are special-purpose software (e.g., GNU Privacy Guard and PGP), file archivers, and even some text editors (e.g., emacs or vi)
- Password protected

3.2.8 Multiple Log-on Restriction Policy

Policy: Individual CSP users are not be able to log on to CSP from more than one workstation at a time, or be able to access client level data (Protected Personal Information) from more than one location at a time.

Explanation: CSP provides the ability to run reports *and download client-level data to local computer networks*. To ensure the security and accountability for such data, users must not be able to log on to more than one workstation at a time.

Procedure: There are two acceptable scenarios for compliance:

1. When user logs on at the 2nd workstation, the system can provide a message notifying the user that they must first log off of the 1st workstation, or

2. When the user logs on at the 2nd workstation, the system can automatically log the user off of the 1st workstation and allow access at the 2nd workstation.

3.2.9 Remote Access Policy

Policy: CSP is intended to be accessed on-site from the CHO's network, desktops, laptops and mini-computers that are web capable.

In special circumstances user access from remote locations may be permitted after application and approval by both the Agency and System Administrators.

The Remote Access Policy and Agreement is an extension of the User Agreement and CSP Policies and Procedures manual. The user shall comply with all Policies, Procedures, Agreements and all rules governing CSP.

The Agency Administrator has the responsibility to assure the user is in compliance with this and all other Policies, Procedures, Agreements and rules governing CSP.

All staff that access CSP remotely must meet the standards detailed in the System Security policies and procedures (see Policy and Procedures) and may only access it for activities directly related to their job.

Examples of Remote Access:

1. CHO offices on secure networks to support agency use of the system.
2. Training Centers on secure networks when providing services or training in the field.
3. Private Home Office on secure networks to provide client assistance and real-time data entry of client data.
4. Agency Administrators or System Administrators only: Private Home Office on secure networks to provide system support as needed.

Explanation: Because CSP enables authorized users to access client-level data via the internet on web-capable devices, remote access must be restricted to authorized personnel and uses only.

Continued on next page.

Procedure: Requirements for Remote Access of CSP include (This policy covers access by individuals under items 3 and 4 above.):

- Remote access will only be allowed on secure networks. (User will not access CSP on any non-protected, free, or other network or Wi-Fi).
- Remote access is allowed only through a Virtual Private Network (VPN)
- Data from CSP will not be downloaded to any remote access site at any time for any reason.
- All CSP data (hardcopy) will be securely stored and/or disposed of in such a manner as to protect the information.
- Monitors need to be equipped with security screens at all times.
- System security provisions will apply to all systems where CSP is accessed and the CHO employing the User will certify such systems for compliance.
- User must certify compliance with all CSP Policies, Procedures and Agreements.
- User must follow all confidentiality and privacy rules.
- User must assure access only for activities directly related to their job.
- User must allow for direct inspection of the remote access location by the Agency Administrator and compliance will be certified by the CHO.
- User must access CSP remotely from a private home office area.
- User must access CSP remotely from a dedicated computer station, used for work purposes only and certified as such by the CHO.
- User must keep Agency Administrator informed of any IP address changes in a timely manner.
- Agency Administrators must inform the System Administrator of any IP address changes in a timely manner.
- Agency and System Administrators must keep an up to date log of Remote Access Users' IP Addresses.

Remote Access Authorization

Application for remote access must be made by completing the CSP Remote Access Agreement and submitting a completed form to the Agency Administrator.

Upon receipt the Agency Administrator will review and confirm the need for the applicant to have remote access. The signed agreement will then be forwarded to the System Administrator for final approval.

The System Administrator will sign and retain the CSP Remote Access Agreement, thus authorizing remote access for the identified user. The System Administrator will advise both the Agency Administrator and the User that approval has been granted.

Violation of this or any CSP policy or agreement may result in the termination of the User License or Agency Participation.

3.3.0 Digital Data Retention Policy

Policy: Client PPI stored on any digital medium is purged, if no longer in use, 7 years after the data was created or last changed (unless a statutory, regulatory, contractual or other requirement mandates longer retention). Also, when digital medium where client PPI has been stored is to be decommissioned, it is reformatted more than once before reusing or disposing of the medium.

Explanation: PPI that is no longer needed must be removed in such a way as to reliably ensure the data cannot be retrieved by unauthorized persons. Because digital medium cannot be reliably erased via single reformatting, multiple (at least twice) reformatting is necessary to ensure the data cannot be retrieved.

Procedure: Every three years digital files where PPI is stored are reviewed and client PPI that is no longer needed is deleted or otherwise removed in such a way as to reliably ensure the data cannot be restored.

At any time digital medium (computers, servers, data storage devices, etc.) where PPI has been stored is to be decommissioned, IT is instructed to reformat the medium at least twice prior to repurposing or disposing of said medium.

4. Standard Operations

4.1 Access to CSP

4.1.1 Agreements

Policy: The Executive Director (or other empowered officer) of any agency wishing to connect to CSP signs an Agreement with CSB before any member of that agency is granted access.

Explanation: Only agencies that have agreed to the terms set out in the Agreement are allowed access to the CSP. The Agreement includes terms and duration of access, an acknowledgement of receipt of the Policies and Procedures Manual, and an agreement to abide by all provisions contained therein.

Procedure: CHOs are given a copy of the Agreement, the location of the Policies and Procedures Manual, and any other relevant paperwork in time for adequate review and signature. Once that paperwork has been reviewed and signed, agency users are trained to use CSP. Once training has been completed, each user is issued a username and password. Signing of the Agreement is a precursor to training and user access.

4.1.2 New User Licenses

Policy: If necessary, CHOs purchase additional User Licenses from Wellsky through the Community Shelter Board. The cost for User Licenses is determined by Wellsky, and is not be changed by the Community Shelter Board.

Explanation: As CHOs grow and the number of CSP users increases, CHOs may need to purchase additional User licenses. This purchase can be made at any time. Licenses are purchased online, through the CSP program, by the user with System Administrator privileges – the CSB Database Administrator. Wellsky then invoices CSB for the cost of the licenses.

Procedure: CHOs wishing to purchase additional User Licenses complete a License Request Form included as an attachment to the CSP Policies and Procedures Manual. The CHO returns this form, with a check to cover the costs of the licenses, to the CSB Database Administrator. The CSB Database Administrator purchases the User Licenses from Wellsky and forwards the check and copy of the request form to the CSB Finance Department for the deposit. The CSB Database Administrator notifies the CHO when the additional licenses are available.

4.1.3 Existing Licenses Redistribution

Policy: CSB conducts an annual reallocation process of unused licenses, to start in May of each year for the next Fiscal Year.

Explanation: Based on the contract that CSB has with Wellsky the annual maintenance fee for each license is $238, while the purchase cost for a new license is $250. Given the high cost of purchasing and maintaining the licenses, it is not feasible for the agencies and CSB to keep a large amount of unused licenses in stock and it is more cost effective to reallocate licenses if they are needed, throughout the system.

Procedure: CSB has an annual reallocation process of unused licenses, to start in May of each year for the next FY, per the following schedule:

Date	Step
May15	Agencies receive email from CSB asking them for number of licenses that agency would need for next FY.
May15 – June 1	Agencies respond back to CSB using the License Relinquishment form, or the License Request Form.
June 5	Agencies receive email from CSB with summary of licenses needed for next FY and the available pool of unused licenses.
June 10 - June 15	CSB re-allocates relinquished licenses to agencies who have requested new licenses for the new FY on a lottery basis, 1 license/agency, based on the available pool, until the pool is exhausted. Re-allocated licenses will be made available on July 1st.
June15 – June 19	If there are still licenses left in the pool, CSB will ask Wellsky to remove these licenses from the CSP contract. If more licenses are needed, the respective agencies will be informed and the licenses ordered from Wellsky. Re-allocated and newly purchased licenses will be made available on July 1st.
July 1	CSB will invoice each agency for the annual maintenance cost, based on the number of current licenses for the upcoming FY, plus the full price for any newly purchased licenses.

At any point in the FY, or if there are no available "reallocation" licenses agencies can purchase new licenses for $250/license. In addition to the "new license fee" the agencies have to contribute the agreed upon annual maintenance fee/license, based on the current number of licenses, starting with the next FY.

4.1.4 CSP License Invoicing

Policy: CSB invoices each agency for each new license at the time of purchase and CSB invoices the applicable annual CSP license support fees at the start of each fiscal year.

Explanation: Wellsky charges a one-time purchase fee for each license due at time of purchase and an annual support fee for each license purchased which they bill on a quarterly basis to CSB .

Procedure: The CSB Database Administrator calculates and submits to the CSB Finance Department the total amount to be invoiced to each agency for applicable license support fees at the beginning of each fiscal year. The applicable fees are re-examined in May of each year per CSB's license redistribution policy. When an agency purchases a new license CSB Database Administrator submits to the CSB Finance Department the total of the one time purchase price to be invoiced to the agency immediately. CSB Database Administrator issues the new license upon receipt of payment from the agency.

4.1.5 User Activation

Policy: Each new user is issued a username and password to access CSP upon approval by the CHO and completion of training directed by the CHO and signing of the CSP User Agreement.

Explanation: CHOs determine which of their employees have access to CSP. Every user must receive appropriate CSP training before being issued a username and password.

Procedure: Agency Administrators distribute user licenses for their CHO, adding and deleting users as needed. The CSB Database Administrator and the Agency Administrators are responsible for training new users. The CSB Database Administrator provides training to Agency Administrators and users and will supplement this training as necessary. The initial username and password are temporary and the user has to be CSP certified within 60 days of his/her CSP access in order to continue operations in CSP.

4.1.6 CSP User License Ownership

Policy: CSB maintains ownership of user licenses when a program terminates or discontinues use of CSP or when CHOs decide to reduce their number of CSP licenses. Licenses are redistributed yearly, through a CSB directed process.

Explanation: CSB retains ownership rights of all CSP user licenses in the event that a program terminates or is otherwise discontinued from CSP participation or when CHOs decide to reduce their number of CSP licenses.

Procedure: When a program discontinues CSP participation or wishes to reduce their number of CSP users/licenses the CSB Database Administrator deletes all user accounts affected and reallocates the licenses back to CSB for termination or redistribution. The CSB Database Administrator is responsible for managing the allocation of all user licenses within CSP.

4.1.7 CSP User Agreements

Policy: Each CHO User signs a CSP User Agreement before being granted access to CSP.

Explanation: Before being granted access to CSP, each user must sign a CSP User Agreement, stating that he or she has received training, will abide by the CSP Policies and Procedures Manual, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in CSP relevant to the delivery of services to people in housing crisis in Columbus and Franklin County.

Procedure: The CHO Agency Administrator distributes CSP User Agreements to new CSP Users for signature. The user signs the CSP User Agreement. The Agency Administrator collects and stores signed CSP User Agreements for all users. The existence of signed CSP User Agreements is verified during the annual CSP on-site review.

4.1.8 CSP User Authorization

Policy: All CSP users are required to have a signed CSP User Agreement on file at CSB. All CSP users are required to have a CSP certification on file at CSB.

Explanation: It is necessary to ensure that only authorized and trained personnel with a signed CSP User Agreement on file with CSB receives access to CSP.

Procedure: Agency Administrators are required to file a signed CSP User Agreement for each user with CSB prior to the user receiving access to CSP. Agency Administrators are also required to delete a user's account and notify CSB immediately by fax or email when a user's need for access changes (i.e. termination or employment, taking a new position, etc.).
CSB's Database Administrator maintains a file for these user agreements and reconciles the active user list in CSP to the hard copy files of signed CSP User Agreement at least once each month. If it is found that there are users in the system that do not have a signed agreement on file those user accounts will be immediately deactivated and an email notification sent to the Agency Administrator. An agency found to be noncompliant in this regard will require corrective action to be taken. For the sake of expedience it is acceptable to fax a copy of the agreement to CSB. The fax should consist of the signed user agreement marked "NEW USER". Agency Administrators and CSB are required to keep a copy of the user's CSP certification on file. No end-user will be permitted to access CSP more than 30-60 (dependent on project type) days, without having CSP certification.

Agency Administrators are authorized to pre-certify end users to get them working in the system quickly. Precertification must include:

- Full training provided by the Agency Administrator or their chosen power-user, utilizing the CSP Training site.
- CSP User Agreement signed by end user and signed by the Agency Administrator and submitted and received by the Database Administrator at CSB.
- End-user signed up for the next applicable CSP Certification training offered by CSB.

4.1.9 CSP User Agreement Breach

Policy: CSB takes corrective action when a breach of the CSP User Agreement is discovered.

Explanation: CSB enforces the Agreements signed by CHO Executive Directors, Agency Administrators, and end users.

Procedure: When a breach is detected the user account of the person or persons involved is immediately deactivated by the CSB Database Administrator and notification sent to the Agency Administrator and/or the Agency Executive Director if necessary. All agency users may be deactivated for a serious breach. The CSB Database Administrator is responsible for notifying the Operations Director and the CSB Executive Director of the agency breach.

4.1.10 Training

Policy: CSB provides adequate and timely CSP training.

Explanation: CSB provides training in the CSP software.

Procedure: The CSB Database Administrator provides training to all new users. Agency Administrators are given additional training relevant to their position. Agency Administrators are expected to train new agency staff with the assistance of the CSB Database Administrator. The CSB Database Administrator provides periodic training updates and refreshers for all users, based on need.

Regular monthly, quarterly or bi-quarterly in-person trainings are scheduled by the CSB Database Administrator for each project type. New CSP users are required to attend in-person training within 60 days from their CSP access. Successful completion of the training and a test will be required for CSP Certification of the user. If the user fails to become certified within 60 days of CSP access, his/her access to CSP will be turned off.

4.2 Data Collection

4.2.1 Required Data Collection/Fields

Policy: CHOs collect and enter into CSP a required set of data variables for each client which is specified in the Agreement.

Explanation: Each Agreement will specify the data elements which must be collected for each client contact. CHOs may choose to collect and enter more client information for their own case management and planning purposes as is permissible under applicable law.

Procedure: The Agreement contains a reference to a listing of data elements to be collected and entered in CSP for each client contact.

4.2.2 Appropriate Data Collection

Policy: CSP users only collect client data relevant to the delivery of services to people in housing crises in Columbus and Franklin County.

Explanation: The purpose of CSP is to support the delivery of homeless and housing services in Columbus and Franklin County. The database should not be used to collect or track information not related to serving people in a housing crisis or planning for the elimination of homelessness.

Procedure: CSP users ask the CSB Database Administrator for any necessary clarification of appropriate data collection. CSB periodically audits pick-lists and agency specific fields to ensure the database is being used appropriately.

4.2.3 CSP Protected Personal Data Collection and Privacy Protection

Policy: CSB and CHO ensure that all required client data will be captured in CSP while maintaining the confidentiality and security of the data in conformity with all current regulations related to the client's rights for privacy and data confidentiality.

Explanation: Clients have the right to expect provider agencies to collect and manage their protected personal data in a manner that is secure and maintains their privacy. Clients have the right to know why agencies are electronically collecting their information and how it will be used.

Procedures:

1. The CHO has a privacy notice sign posted at each intake desk, minimally the one provided by CSB. The sign is posted in an area accessible and easily viewed by clients.
2. The CHO has a written privacy policy, minimally the one provided by CSB, to cover the electronic data collection, use and maintenance of the client's protected personal information. Clients are made aware of the privacy policy. The policy is posted on the agency's website and shared with the client upon request. The policy is reviewed at least annually and updated as needed.
3. The CHO presents each client with a Client Acknowledgement for Electronic Data Collection form and informs the client about the provisions of the form. The CHO attempts to obtain a signed Client Acknowledgement for Electronic Data Collection form from each client before data is entered into the database and maintains this form on file at the agency, in the client's file.
4. In case the acknowledgment form is not signed, the CHO still has to electronically collect in CSP any and all CSP required data elements provided by the client to the agency. Based on current HUD regulations, CSB does not require client consent for the electronic data collection. The agency may also elect to implement a more restrictive client privacy policy than the one provided by CSB with respect to other data that is not CSP required.
5. If the CHO has a more restrictive privacy policy than the one provided by CSB that disallows the collection and/or entry of the protected personal information (name, birth date and social security number) in CSP without written client consent and the client refuses to provide written consent, the agency must enter the data by creating an Unnamed record for tracking purposes. This is a function within CSP which involves entering the client's protected personal information (name, birth date and social security number) which the system then uses to create a unique record identifier. The system then strips PPI out of the record. If the client consents with the electronic data collection, the agency must electronically collect in CSP any and all CSP required data elements provided by the client to the agency. Generally, the more restrictive CSP related privacy policy should be implemented only by agencies that by law are required to have privacy standards more restrictive than the HUD standards (i.e. HIPAA, etc).
6. The agency must provide CSB with its client privacy policy at the beginning of each CSB program year, with any updates made throughout the previous program year.

4.2.4 Educating Clients of Privacy Rights

Policy: The Agency Administrator maintains a current privacy policy and a privacy notice which includes the uses and disclosures of information.

Explanation: Clients have a right to expect service agencies to collect and manage their protected personal data in a manner that is secure and maintains their privacy.

Procedure: The Agency Administrator ensures that a written privacy policy and a privacy notice is in place and up to date. The Agency Administrator also ensures that the privacy notice is posted in an area accessible and easily viewed by clients. The clients are informed of their rights under the privacy policy and receive the policy if requested. This policy is reviewed at least annually and updated as needed. CSB provides, as part of the Policies and Procedure Manual, the most current Privacy Policy and Privacy Notice. The CHOs should minimally adopt the documents provided by CSB.

4.2.5 Scanned Document Management

Policy: CSB is responsible for organization and management of the CSP. It is necessary to standardize the way the document upload feature is utilized in order to ensure the information uploaded is usable system-wide.

Explanation: CSB desires that essential client documentation be scanned and uploaded to CSP. CSP, as a client document repository is a useful tool to case managers helping clients exit quickly from emergency shelters into stable housing. Client documentation is available quickly, avoiding delays in client services.

Procedure: CSB seeks to provide a uniform CSP which yields the most consistent data for client management, agency reporting, and service planning. To this end, CSB is providing the following standards as guidelines for the utilization of the document upload feature.

Classification of Uploaded Documents:

- Permanent Documents (Birth Certificate, Social Security Card, Photo ID, Certification of Disability, etc.)
- Temporary Documents (DCA Applications, Point-In-Time Eligibility Determination Documentation, etc.)

Security on Uploaded Documents:

- Permanent Documents OPEN
- Temporary Documents CLOSED

Documents to be uploaded:

- Only documents relevant to achieving a goal plan and needed for accessing housing and services should be uploaded, for example DCA Applications.
- Avoid duplication; if the document is already uploaded don't upload again.

Naming Standards for uploading documents:

- Format: Client ID#. Document Title. Date Saved
- Example: 77045. DCA Application Rent and Deposit. 120409

Uploaded Document retention:

- Permanent Documents: In perpetuity or until client profile is inactive for 7 years or more as per the current data archiving standard.
- Temporary Documents
  - DCA Applications will be deleted by CSB DCA Program Manager once downloaded.
  - Other: deleted by provider when client exits the program.
- Older documents should not be deleted when an updated version is uploaded.

4.3 Data Entry

4.3.1 Shelter Data Entry (applies only to emergency shelters)

Policy: The ShelterPoint module in CSP is meant to serve as a tracking tool for actual shelter bed use. Clients admitted in shelter are entered in ShelterPoint.

Explanation: To ensure consistency in how emergency shelter beds are used, all clients admitted into the emergency shelter are entered in CSP, via the ShelterPoint module.

Procedure: All clients served by the shelter must be entered into CSP and ShelterPoint.

- Clients who receive overnight accommodation must be checked into ShelterPoint no later than 9:00 a.m. the next day.
- All clients who do not return for shelter (no show) or who otherwise did not use their bed (e.g. out on pass) MUST BE CHECKED OUT of ShelterPoint by 9:00 a.m. the next morning.
- Client status in ShelterPoint *must not be changed* between 9:00 a.m. to 11:00 a.m., Monday through Friday, as this is when CSB will be generating reports from ShelterPoint for the prior evening.
    - The report that is generated by CSB each day is called the Daily Bedlist Report. It is the Agency Administrator's task to review this report each day and verify the accuracy of the numbers posted.
    - Agency Administrators should notify CSB promptly when inaccuracies in the Daily Bedlist Report are identified and give an estimated time for corrections within CSP to be completed.
- Clients who exit the shelter, after having slept in a bed the previous night, must only be checked out of ShelterPoint and have an exit date entered in CSP *after* 11:00 a.m.

Example

John Doe receives an intake and begins his stay at the shelter on Monday. On Wednesday evening he misses curfew and is a no show. He returns on Thursday at 6:00 p.m. and is readmitted to the shelter and then exits the following Monday.

In this situation,

- Mr. Doe will be entered into CSP and ShelterPoint on Monday (by no later than 9:00 a.m. Tuesday morning). If for some reason data entry cannot be done real-time it will be necessary to back-date the record to the client's actual date and time of entry.
- Since he didn't return Wednesday evening, he would be checked out of ShelterPoint Thursday, no later than 9:00 a.m. (the system will automatically apply the Exit to the client's EntryExit record as well.)
- After returning on Thursday he is then checked back into ShelterPoint (and CSP if exited previously) no later than Friday at 9:00 a.m.
- The following Monday, he is checked out from ShelterPoint on Monday (after 11:00 a.m.).

4.3.2 Customizations

Policy: CHOs have the option of collecting additional data elements in CSP.

Explanation: Custom, additional assessments may be created by the CSB Database Administrator at the request of CHO. Custom assessments contain questions that will be used to collect the additional data elements.

Procedure: CSB Database Administrator, at the request and in collaboration with the Agency Administrators will create custom assessments for CHOs.

4.3.3 Additional Customization

Policy: CHOs purchase any additional database customization directly from Wellsky. CSB does not provide additional customizations. However any proposed customizations must be approved by CSB.

Explanation: It is the responsibility of individual agencies to determine the best way to use CSP for internal data collection, tracking, and reporting. This may include purchasing additional customization directly from Wellsky. CSB must review and approve any proposed customizations to ensure the integrity of the overall system.

Procedure: CHOs provide a proposal to CSB and contact Wellsky directly with additional customization needs.

4.3.4 Data Corrections

Policy: Data should not be changed once the System and Program Indicator Report (SPIR) has been published.

Explanation: Once data has been found compliant through the quarterly Quality Assurance review process the data is then utilized for funder, Continuum of Care, Board and Community Reporting. To maintain the integrity of this reporting it is necessary to be able to provide numbers and statistics consistently over time.

CSB data entry standards require that all data is completely and accurately entered in CSP by the 4th working day of the month after which there is a period of Quality Assurance reviews. It is the Agency Administrator's responsibility that data is entered completely and accurately on an ongoing basis through agency-level QA policies and procedures.

If data is found to be incomplete or incorrect during the QA period it is permissible to make changes up through the last day of the designated cure period. After compliance has been achieved no changes or corrections to the data which has been reviewed should be necessary.

Procedure: Agency Administrators facilitate efficient and accurate data entry through training and monitoring of data entry personnel. Agency Administrators ensure data is accurately entered in a timely manner through rigorous quality assurance practices. If an agency discovers data inconsistencies after the quarterly QA period, the Agency Administrator should contact CSB's Database Administrator. In agreement with CSB's Database Administrator, changes may be allowed to data.

4.3.5 Annual Data Freeze

Policy: Annually, as of October 1st no changes are allowed to data records which have an exit date on or before the last day of the previous fiscal year. The fiscal year data is effectively "frozen" on an annual basis.

Explanation: Once data has been found compliant through the quarterly and annual Quality Assurance review process the data is then utilized for funder, Continuum of Care, Board and Community Reporting. To maintain the integrity of this reporting it is necessary to provide consistent historical numbers and statistics over time.

CSB data entry standards require that all data is completely and accurately entered in CSP by the 4th working day of the month after which there is a period of Quality Assurance reviews. At the end of a fiscal year, data for the entire year as well as the final quarter is reviewed for QA. It is the Agency Administrator's responsibility that data is entered completely and accurately on an ongoing basis through agency-level QA policies and procedures.

If CSB and/or agencies discover a major inconsistency in previous fiscal year's data after October 1st the anomaly will be reviewed by CSB and action decided on a case by case basis.

Procedure: Agency Administrators ensure through staff training and communication that changes will not be made to previous fiscal year data as of October 1st. Agency Administrators facilitate efficient and accurate data entry through training and monitoring of data entry personnel. Agency Administrators ensure data is accurately entered in a timely manner through rigorous quality assurance practices. If an agency discovers data inconsistencies in the previous fiscal year's data after the October 1st cutoff date, the Agency Administrator should contact CSB's Database Administrator. The anomaly will be reviewed by CSB and action decided on a case by case basis.

4.3.6 Data Entry for Couples in Supportive Housing Programs

Policy: Data entry practices correspond with the target population of Supportive Housing programs/units.

Explanation: *Couples present a challenge in data entry and reporting. The Columbus community encourages programs to serve couples, wherever possible, in the supportive housing programs.*

Procedure: For Permanent Supportive Housing units, an eligible client may share a unit with a non-eligible client. Because only the homeless, eligible clients must be accounted for, the couples are entered in CSP as a household with the eligible client as the head of household. By the same token, if both members of the couple are eligible clients, then both need to be entered in CSP and reported on as individuals.

4.4 Quality Control

4.4.1 Data Integrity

Policy: CSP users are responsible for the accuracy of their data entry.

Explanation: Individual users are responsible for the accuracy and quality of their own data entry.

Procedure: In order to test the integrity of the data contained in CSP, the CSB Database Administrator performs regular data integrity checks in CSP. Any patterns of error are reported to the Agency Administrator. When patterns of error have been discovered, users are required to correct data entry techniques and will be monitored for compliance.

4.4.2 Data Integrity Expectations

Policy: CHOs provide the following levels of data accuracy and timeliness:

- All data entered is accurate.
- Entry Dates and Exit Dates must match intake and exit forms within the client file and must be completed for each individual served.
- Blank, "Client Doesn't Know", "Client Refused", and "Data Not Collected" entries do not exceed, collectively, 5% per data field, per month.
- Data entry is completed in CSP as real-time as possible. Data entry for shelter stays is completed by 9am each day for the previous night. Data entry for all other services provided is entered within 48 hours. Allowing for quality checks and corrections for any given calendar month-end, these must be completed within CSP by the fourth working day of the following calendar month.

Explanation: Users enter client data as provided by the client and, preferably, confirmed by documentation. Of the fields required in the Agreement, less than 5% of fields will be left blank or marked as "Client Doesn't Know", "Client Refused", or "Data Not Collected" in one month. For example, if the last zip code field is left blank for 2% of clients, then the last zip code field should not have more than 3% of "Client Doesn't Know", "Client Refused", or "Data Not Collected" responses for clients entered during one month. When service records are added, no services are entered by programs that do not provide that type of service. For example, rental assistance should not be entered by a program that only provides emergency shelter. When service records for shelter stays are added, the client must meet the most basic requirements of the program listed as providing shelter. For example, no clients listed as women should have shelter stays in shelters restricted to men. Agencies strive to complete entry data as real-time as possible. Data entry for shelter stays is completed by 9am each day for the previous night. Other services and items are entered within 48 hours of provision. Data entry for all services provided in one month must be accurately entered into CSP by the fourth working day of the following month. For example, if April 30th falls on a Friday, data for April must be completed by close of business Thursday, May 6.

Procedure: The CSB Database Administrator performs regular data integrity checks in CSP. Any patterns of error at a CHO are reported to the Agency Administrator. When patterns of error have been discovered, users are required to correct data entry techniques and will be monitored for compliance.

4.4.3 Quality Assurance

Policy: CSB performs at least a quarterly quality assurance process for data entered by each CHO, related to CSP.

Explanation: To keep the data integrity at the program and system level, CHOs and CSB perform a quality assurance process, at least quarterly, for data entered in CSP.

Procedure:

All agencies are required to run monthly the Client Duplicate report and inform the CSB Database Administrator of any client duplicates found, by the 4th working day following the end of a month (by fax). This report becomes an integral part of the Monthly/Quarterly quality assurance process.

The Monthly QA review roster is based on the results of the initial run of the preceding Quarterly QA run. If an agency receives a noncompliant rating on the initial run of a quarterly QA review that agency will receive monthly reviews for the next two months.

- **The purpose of the Monthly QA is to encourage Agency Administrators to monitor their compliance status and catch problems early. We are also looking to focus an agency's attention on the QA problems.**
- Review for the previous month is run by the Agency Administrator by the 5th working day of the month.
- Results are distributed (or emailed) to CSB Database Administrator by the 6th working day of the month.
- Administrators are expected to set their own schedule to review and effect a cure prior to the end of the third month of the quarter.
- Agencies will not have to do a monthly report for the third month of each quarter as this is when the Quarterly QA is run.

The Quarterly QA review schedule is 2-tiered:

- For the initial run, the Agency Administrator receive compliance results.
    - **The purpose of this step is to help Agency Administrators in determining the data integrity problems from the previous quarter and allow them sufficient time to correct the errors prior to inclusion in community reports.**
    - Review is run by the Agency Administrator by the 9th working day of the month following the end of the quarter.
    - Summaries are distributed (emailed or faxed) to the CSB Database Administrator by the 10th working day of the month.
    - Non-compliance will result in the Agency Administrator receiving a Non-Compliance email on the 11th working day of the month.
    - Non-compliant agencies are given **5** working days to cure.

- All noncompliant agencies on this run will be added to the Monthly QA Roster.
- Compliance will result in a formal letter addressed to the Agency Administrator and their Executive Director.

- The 2nd run is only for those agencies found non-compliant in the 1st run; Agency CSP Administrator and Executive Director receive the results.
  - **The purpose of the 2nd run is to make sure that all agencies are compliant with the minimal CSB data quality standards which in turn allow us to present the agency and system data in community reports and help the planning process to cover the ongoing homelessness related needs of our community.**
  - CSB Database Administrator will do the 2nd review on the 17th working day of the month.
  - Results are distributed within 3 working days.
  - Compliance will result in a formal letter addressed to the Agency Administrator and their Executive Director.
  - Non-compliance results in a hard-breach letter being issued and signed by CSB's Executive Director.

Any agencies receiving a hard-breach letter may have funding suspended until a cure has been achieved. CSB will not include that agency's data in the Quarterly and/or Semi-Annual System and Program Indicator Report (SPIR) and the program will be issued a "program of concern". The System Results in the SPIR will be revised after the agency becomes compliant. Agency results will NOT be changed.

CSB will not include the agency data in the SPIR or any other reports if CSB staff is not confident in the reliability of that particular agency's data in CSP, independent of the QA results.

CPOA and Quality Assurance Accountability
The Coordinated Point of Access (CPOA) staff collects and enters the majority of the required data elements for each emergency shelter client, however all serving agencies remain accountable for the accurate representation of the client's data within CSP. Programs receiving clients directed to their shelters via CPOA must review all required data elements and ensure all are entered and accurate as of the client's entry. When shelter staff discover an omission or mistake it should be promptly reported to CPOA for entry or correction as needed. Proof of this report should be included in the client's file.

4.4.4 On-Site Review

Policy: CSB performs annual on-site reviews at each CHO of data processes related to CSP.

Explanation: On-site reviews enable CSB to monitor compliance with the Policies and Procedures Manual and Agreements.

Procedure: This review is part of the Annual Program Review and Certification process. The Monitoring Guide for Sub-recipients Program Review & Certification details the annual on-site review.

4.5 Data Retrieval

4.5.1 Contributing HMIS Organizations (CHOs)

Policy: CHOs have access to retrieve any individual and aggregate data entered by their own programs. CHOs do not have access to retrieve aggregate data for other agencies or system-wide.

Explanation: Any data entered within an agency is available for reporting. Data entered by other agencies is not available, unless there are explicit data-sharing agreements in place.

Procedure: When using the report writer, ART or Qlik modules, users are only able to extract data from those records to which they have access. These modules will limit user access and only report data from records to which the individual user has access.

4.5.2 CSB Access

Policy: The Community Shelter Board has access to retrieve all data in CSP. CSB does not access individual client data for purposes other than direct client service-related activities, reporting, maintenance, and checking for data integrity, with the exception of compliance with local or federal law enforcement warrants.

Explanation: CSB Data & Evaluation and Programs and Planning departments have access to all data in the database. No other staff member of CSB has access to client-level data. CSB protects client confidentiality in all reporting.

Procedure: CSB's Operations Director is responsible for ensuring that no individual client data is retrieved for purposes other than direct client service, reporting, maintenance, and performing data integrity checks. CSB's Operations Director will oversee all reporting for the CSB.

4.5.3 Public Access

Policy: CSB addresses all requests for data from entities other than CHOs or clients. Individual client data is provided, upon request, to the CHO which entered the data, CSB's funder for the specific program for which individual client data is requested, outside organizations under contract with CSB for research, data matching, and evaluation purposes, or the client him or herself. Proper authorization is required for all requests.

Explanation: Any requests for reports or information from an individual or group who has not been explicitly granted access to CSP will be directed to CSB. No individual client data is provided to meet these requests without proper authorization.

Procedure: All requests for data from anyone other than a CHO or a client are directed to the CSB Database Administrator. It is CSB's policy to provide aggregate data on homelessness and housing issues in Columbus and Franklin County. CSB also issues periodic public reports about homelessness and housing issues in Columbus and Franklin County. No individual client data is reported in any of these reports. CSB may share client level data with contracted entities as follows: CSB's funder for the specific program for which individual client data is requested, outside organizations under contract with CSB for research, data matching, and evaluation purposes. The results of this analysis are always reported in aggregate form, client level data is not publicly shared under any circumstance.

4.5.4 Data Retrieval Support

Policy: Agencies create and run agency-level reports. CSB provides its own reports to agencies for their own use.

Explanation: The Agency Administrator has the ability to create and execute reports on agency-wide data. This allows agencies to customize reports and use them to support agency-level goals.

Procedure: The Agency Administrator is trained in reporting by Wellsky or by the CSB Database Administrator. CSB's Database Administrator provides the template for reports specifically required by the Community Shelter Board. CSB's Database Administrator is a resource for report creation.

4.5.5 Appropriate Data Retrieval

Policy: CSP users only retrieve client data relevant to the delivery of services to people in housing crises in Columbus and Franklin County.

Explanation: The purpose of CSP is to support the delivery of homeless and housing services in Columbus and Franklin County. The database should not be used to retrieve or report information not related to serving people in a housing crisis.

Procedure: Agency Administrators ask the CSB Database Administrator for any necessary clarification of appropriate data retrieval.

4.5.6 Inter-Agency Data Sharing

Policy: Data included in the Profile, EntryExit, and Service Transaction section of a client record is viewed by all users with the exceptions below. CHOs determine the security settings of the additional information entered in CSP.

Explanation: When new clients and new service records are entered into CSP, the information, by default is open to be viewed by users from other CHOs. Open sections of the record can be seen and changed by users from another CHO. There are a few agencies that are regulated by HIPAA Standards and those Agencies' records, by default, are closed. Closed sections of the record can neither be seen nor changed by users from another CHO. Regardless of status, all sections of each record will appear in aggregate reports

Currently, the following are the agencies that are entering and sharing information in CSP:

Alvis, Inc.	Huckleberry House	The Salvation Army
Community Housing Network	Lutheran Social Services/Faith Mission	U.S. Department of Veteran's Affairs
Equitas Health	Maryhaven	Volunteers of America of Greater Ohio
Gladden Community House	National Church Residences	YMCA
Homeless Families Foundation	Netcare Access	YWCA
	Southeast, Inc.	

Procedure: It is the intent of CSB to allow as much data sharing as appropriate and necessitated by the clients' needs and the services provided to meet those needs. Client profiles are set as "Open", as are Service Transactions and EntryExit records. HIPAA regulations, as followed by some of the CHOs take precedence over the above Policy and Procedure. HIPAA regulated agencies will have all their clients' data CLOSED.

4.5.7 Agency Data Sharing

Policy: CHOs can share their data for research and data analyses purposes with prior approval by CSB.

Explanation: CSP provides the ability to run reports and download client-level data by all CHOs. CHOs are encouraged to analyze their data and make programmatic decisions based on the information contained in CSP. Data sharing must be done in conjunction with careful consideration of data confidentiality and privacy protocols.

Procedure: The following steps are required by each CHO that wishes to share its data with an external contractor or vendor for research and data analysis purposes:

1. Data sharing will have to be approved by CSB
2. The provider will have to submit to CSB the data sharing agreement that will need to contain, at the minimum:
    a. Scope of the analysis/research that must be limited to the data that pertains to the individuals served by provider
    b. Information transmittal protocols
    c. Data confidentiality/privacy protocols
    d. Data handling after the analysis/research is complete

4.6 Contract Termination

4.6.1 Initiated by CHO

Policy: The termination of the Agreement by the agency will affect other contractual relationships with the CSB. In the event of termination of the Agreement, all data entered into CSP remains an active part of CSP, and records keep their original security settings.

Explanation: While agencies may terminate relationships with CSB and CSP, the data entered remains part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in Columbus and Franklin County. The termination of the Agreement will affect any other contractual relationships with CSB.

Procedure: Partner Agencies are required to participate in CSP as a condition of their funding. For Partner Agencies, termination of the Agreement will be addressed in the context of the larger contract with CSB. For the Other CHOs terminating the Agreement, CSB will need to receive official notification with a date of termination of the Agreement. The Executive Director of CSB will notify the CSB Database Administrator. In all cases of termination of Agreements, the CSB Database Administrator will inactivate all users from that CHO on the date of termination of the Agreement.

4.6.2 Initiated by the Community Shelter Board

Policy: CSB will terminate the Agreement for non-compliance with the terms of that contract upon 30 days written notice to the CHO. CSB will require any CSP violations to be rectified before the Agreement termination is final. CSB may also terminate the Agreement with or without cause upon 30 days written notice to the CHO and according to the terms specified in the Agreement. The termination of the Agreement by CSB may affect other contractual relationships with the CSB. In the event of termination of the Agreement, all data entered into CSP will keep their initial security settings.

Explanation: While CSB may terminate the Agreement with the CHO, the data entered by the CHO prior to termination of contract remains part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in Columbus and Franklin County. The termination of the Agreement may affect other contractual relationships with the Community Shelter Board.

Procedure: CSB Partner Agencies are required to participate in CSP as a condition of their funding. For Partner Agencies, termination of the Agreement will be addressed in the context of the larger contract with CSB. When terminating the Agreement, the Executive Director of CSB will notify the CHO at least 30 days prior to the date of contract termination. The Executive Director of CSB will also notify the CSB Database Administrator. In all cases of termination, the CSB Database Administrator will inactivate all users from that CHO on the date of contract termination.

4.7 Programs in CSP

4.7.1 Adding a New Program in CSP

Policy: Agency Administrators follow the prescribed procedure to notify CSB 's Database Administrator prior to implementing a new program within CSP. The CSB Database Administrator follows a standard formula when naming a new program within CSP.

Explanation: When a new program is to be added or activated within CSP the Agency Administrator is required to submit the requested information via the provided form prior to implementation. The CSB Database Administrator follows a standard pattern when creating a name for new programs being added to the CSP and obtains approval from the Data & Evaluation department prior to implementation.

Procedure: When a new program is to be added or activated within the CSP, the following steps occur:

1. At least 60 days prior to the anticipated implementation date, Agency Administrators complete a "CSP Program Implementation Request Form" and submit to the CSB Database Administrator.
2. If being newly added in CSP, the CSB Database Administrator ensures that the following standard formula is used when creating a name within CSP:
   Agency (Abbreviation) – CSB Contract/Program Name
   Example:
   CSB Test Program
3. The CSB Database Administrator present the completed request form and recommended program name to the Data & Evaluation Department for review and approval.
4. The CSB Database Administrator notifies the Agency Administrator of approval status at least 30 days prior to the requested CSP implementation date.
5. The CSB Database Administrator assists the Agency Administrator with the CSP implementation as needed.

4.7.2 Making Changes to Existing Programs

Policy: The Agency Administrator notifies the CSB Database Administrator of programmatic changes per the procedure below.

Explanation: Agencies must notify CSB of any program changes which affect data collection, data entry, data quality and/or data reporting. Agency Administrators accomplish this via the provided form which requests details such as (but not limited to) funding status, program type, quality assurance participation, program start and end date, capacity, bedlist specifications etc.

Procedure:

1. The Agency Administrator notifies the CSB Database Administrator of any applicable programmatic changes to existing programs which may have an effect on data collection, data entry, data quality or data reporting (i.e. program expansion of capacity or scope; termination; deactivation; discontinuance of CSP participation, etc.) Notification is made in writing at least 45 business days before the proposed implementation date of the change.
2. CSB's Database Administrator will circulate the completed form to the Data & Evaluation Department for review & comment.
3. Recommendations and timeline for assistance are returned to the agency no fewer than 10 business days prior to the requested implementation date.
4. The CSB Database Administrator assists with changes within CSP as necessary.

While the Agency Administrators have the access to make changes to programs within the system, it is required that any changes first be reviewed with the CSB Database Administrator to determine the overall effect of the changes and to allow for documentation of changes as well as the arrangement of any necessary support.

4.7.3 Maintaining a CSP Program Matrix

Policy: The CSB Database Administrator maintains a complete and up to date Program Matrix of CSP.

Explanation: The Program Matrix is a complete index of all programs existing in CSP, their status and other details such as (but not limited to) funding status, program type, quality assurance participation, program start and end date, etc.

Procedure: The CSB Database Administrator records changes being made to any existing program in CSP (termination, deactivation, etc.) and the addition of the new programs via the Program Matrix, upon receipt of the proper documentation from the Agency Administrator and after the finalization of the implementation plan. The CSB Database Administrator is responsible for ensuring the Program Matrix reflects any and all changes to programs within CSP. The CSB Database Administrator reviews the Program Matrix with the Data & Evaluation Department on a monthly basis.