CSP

Policies and Procedures

Welcome to the World of CSP

If you work in a helping agency serving those in need, you probably do not do it for the money - you do it because you want to make a difference in the world. Technology should help you make that difference, not keep you tangled in red tape.
CSP will help you make a difference in the lives of men, women, and children who come into your agency. It's specifically designed to make sure your clients receive the best, most complete service possible. While it can't give anyone a home or the services they need, it does bring together the agencies and people who can. Through technology, CSP creates a community of care and a virtual one-stop entry point for client services.
As a computerized data collection tool CSP is specifically designed to capture client-level, system-wide information on the characteristics and service requirements of the men, women, and children experiencing need. In plain language, it helps agencies share relevant, up-to-date information on clients and service availability (i.e. available beds, program eligibility, etc.).

Federal Requirements

Carroll County, MD is developing a Community Management Information System (CMIS) utilizing Bowman Internet System's internet-accessed ServicePoint software to best serve a wide variety of our clients' needs. Originally conceived to meet Congress' mandate to the Department of Housing and Urban Development (HUD) for data and analysis on the extent of homelessness and the effectiveness of McKinney-Vento funded programs, the CMIS and CSP will fulfill HUD's directives that, to remain eligible to receive grant awards, all federally-funded jurisdictions:

- Develop unduplicated counts of clients served at the local level
- Analyze patterns of use of persons entering and exiting the homeless assistance system
- Evaluate the effectiveness of these systems

Additionally, CSP's flexibility and robustness allows it to be used for eligibility, intake, case management, follow-up, data collection and reporting that non-homeless centered agencies also find useful. Because many service-centered agencies can use the system, Carroll County's Circle of Caring Homeless Board CMIS Steering Committee (now the CSP Steering Committee) chose "Community ServicePoint" to identify both the software's homeless element and its broader uses.

The CSP Steering Committee has adopted the following:

CSP Mission Statement: Community ServicePoint will provide standardized, timely information through a coordinated system that improves access to housing, community services, and resources for the people of Carroll County.
CSP Goals:

- To meet HUD's requirements that every Continuum of Care have a Homeless Management Information System (HMIS) in place by September 2004.
- To develop new means of collaboration to help agencies work together in new and creative ways to support solving the common needs of clients in Carroll County.
- To ensure a continuity of care, ensuring each client receives the highest, most holistic level of care possible.
- To speed a person's access to needed resources helping clients get the services they need.

Governing Principles

Described below are the overall governing principles upon which all other decisions pertaining to the CSP are based.

Data Integrity: Data are the most valuable assets of the CSP. It is our policy to protect this asset from accidental or intentional unauthorized modification, disclosure or destruction.

Access to Client Records: The Client Records Access policy is designed to protect against the recording of information in unauthorized locations or systems. Only staff who work directly with clients or who have administrative responsibilities will receive authorization to look at, enter, or edit client records. Additional privacy protection policies include:

- No client records will be shared electronically with another agency without written client consent;
- Client has the right to not answer any question, unless entry into a service program requires it;
- Client has the right to know who has added to, deleted, or edited their client record;
- Client information transferred from one authorized location to another over the web is transmitted through a secure, encrypted connection.

Application Software: Only tested and controlled software should be installed on networked systems. Use of unevaluated and untested software outside an application development environment is prohibited.

Computer Crime: Computer crimes violate state and federal law as well as the CSP Data Security Policy and Standards. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly or criminally liable for their actions, or both. CSP staff and authorized agencies must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it. Copyrighted software must not be loaded or used on systems for which it is not licensed.

End User Ethics: Any deliberate action that adversely affects the resources of any participating organization or institution or employees is prohibited. Any deliberate action that adversely affects any individual is prohibited. Users should not use CSP computing resources for personal purposes. Users must not attempt to gain physical or logical access to data or systems for which they are not authorized. Users must not attempt to reverse-engineer commercial software. Users must not load unauthorized programs or data onto CSP computer systems. Users should scan all personal computer programs and data for viruses before logging onto CSP computer systems.

SECTION 1:

Contractual Requirements and Roles

SOP#: CRR-001 Prepared by: CSP Effective date: 06/04

Title: CSP CONTRACT REQUIREMENTS

Policy: CSP is committed to provide services to participating agencies.

Standard: CSP will provide quality service to new and existing participating agencies.

Purpose: To outline the basic services for existing and new agencies

Scope: Participating agencies and CSP

Basic Requirements:

A. Purchase of Software Licensing and Technical Support: All existing and new sites participating in the CSP that are funded through Carroll County Dept of Citizen Services will have most costs covered by their contractors include user licenses for ServicePoint and technical assistance provided by CSP staff. Please note: Participating Agencies are responsible for all costs associated with hardware acquisition and maintenance, personnel, and Internet access.

Agencies that are not funded to participate in the CSP through a Continuum of Care contract or exceed their license allotment must pay a yearly fee according to CSP's cost document.

B. Access: Existing and new Participating Agencies covered under existing Contacts will not be granted access to the ServicePoint software system until a contractual agreement has been signed with CSP.

SOP#: CRR-002 Prepared by: CSP Effective date: 06/04

Title: STEERING COMMITTEE

Policy: A Steering Committee, representing all stakeholders to this project will advise all project activities.

Standard: The responsibilities of the Steering Committee will be apportioned according to the information provided below.

Purpose: To define the roles and responsibilities of the project Steering Committee.

Scope: All project stakeholders

Responsibilities:

The Steering Committee advises and supports CSP's operations in the following programmatic areas: fundraising and resource development; consumer involvement; and quality assurance/accountability. The committee meets quarterly.

Membership of the Steering Committee will be established according to the following guidelines:

- Target for membership will be 25 persons;
- There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the project;
- There will be a pro-active effort to fill gaps in the membership of the Committee in terms of constituency representation: consumer representatives, shelters for families and individuals, advocacy organizations, and government agencies that fund homeless assistance services, and statewide geographic distribution.

The CSP Steering Committee is fundamentally an advisory committee to the CSP. However, the CSP staff delegates final decision making authority to the Committee on the selected key issues that follow. These issues include:

- Determining the guiding principles that should underlie the implementation activities of CSP and participating organizations and service programs;
- Selecting the minimal data elements to be collected by all programs participating in the CSP.
- Defining criteria, standards, and parameters for the release of aggregate data; and
- Ensuring adequate privacy protection provisions in project implementation.

SOP#: CRR-003 Prepared by: CSP Effective date: 06/04

Title: **CSP MANAGEMENT**

Policy: A CSP management structure will be put into place that can adequately support the operations of the CSP state-wide system according to the Guiding Principles described in the Introduction.

Standard: The responsibilities of the CSP staff will be apportioned according to the information provided below.

Purpose: To define the roles and responsibilities of the CSP staff.

Scope: System wide

CSP Roles and Responsibilities: Management:

The CSP coordinator is responsible for oversight of all day-to-day operations including: technical infrastructure; planning, scheduling, and meeting project objectives; Guiding Principles and Policies and Procedures. CSP Coordinator reports to the CSP Manager.

Technical Assistance:

The CSP Coordinator is responsible for overseeing usage of the application ServicePoint and being available for phone support as needed.

Responsibilities and Duties include:

* Provide training on a regular basis to agency staff
* Provide technical assistance and troubleshooting as needed
* Provide technical assistance in generating funder-required reports

Data Analysis:

CSP's data analysis team is responsible for the following:

* Provide data quality queries to sites on a regular basis.
* Provide detailed countywide reports on families and individuals accessing emergency shelter.

Systems Administration / Security / User Accounts:

CSP has a contract with Bowman Internet Systems to host the central server. They will have overall responsibility for the security of the system.

All Agency Administrator user accounts are the responsibility of the CSP staff. All Participating Agency staff user accounts are the responsibility of the Agency Administrator.

SOP#: CRR-004 Prepared by: CSP Effective date: 06/04

Title: ROLE: PARTICIPATING AGENCY EXECUTIVE DIRECTOR

Policy: The Executive Director of each Participating Agency will be responsible for oversight of all agency staff who generate or have access to client-level data stored in the system software to ensure adherence to the CSP standard operating procedures outlined in this document.

Standard: The Executive Director holds final responsibility for the adherence of his/her agency's personnel to the CSP Guiding Principles and Standard Operating Procedures outlined in this document.

Purpose: To outline the role of the agency Executive Director with respect to oversight of agency personnel in the protection of client data within the system software application.

Scope: Executive Director in each Participating Agency

Responsibilities:

The Participating Agency's Executive Director is responsible for all activity associated with agency staff access and use of the ServicePoint data system. This person is responsible for establishing and monitoring agency procedures that meet the criteria for access to the ServicePoint Software system, as detailed in the Policies and Procedures outlined in this document. The Executive Director will be held accountable for any misuse of the software system by his/her designated staff. The Executive Director agrees to only allow access to the ServicePoint software system based upon need. Need exists only for those staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

The Executive Director also oversees the implementation of data security policies and standards and will:

1. Assume responsibility for integrity and protection of client-level data entered into the ServicePoint system;
2. Establish business controls and practices to ensure organizational adherence to the CSP Policies and Procedures;
3. Communicate control and protection requirements to agency custodians and users;
4. Authorize data access to agency staff and assign responsibility for custody of the data;
5. Monitor compliance and periodically review control decisions.

SOP#: CRR-005 Prepared by: CSP Effective date: 06/04

Title: ROLE: PARTICIPATING AGENCY: AGENCY ADMINISTRATOR

Policy: Every Participating Agency must designate one person to be the Agency Administrator.

Standard: The designated Agency Administrator holds responsibility for the administration of the system software in his/her agency.

Purpose: To outline the role of the Agency Administrator

Scope: Participating Agencies

Responsibilities:

The Participating Agency agrees to appoint one person as the Agency Administrator. This person will be responsible for:

- Editing and updating agency information
- Granting access to the software system for persons authorized by the agency's Executive Director by creating usernames and passwords;
- Training new staff persons on the uses of the ServicePoint software system including review of the Policies and Procedures in this document and any agency policies which impact the security and integrity of client information.
- Ensuring that access to the ServicePoint system be granted to authorized staff members only after they have received training and satisfactorily demonstrated proficiency in use of the software and understanding of the Policies and Procedures and agency policies referred to above.
- Notifying all users in their agency of interruptions in service

The Agency Administrator is also responsible for implementation of data security policy and standards, including:

- Administering agency-specified business and data protection controls
- Administering and monitoring access control
- Detecting and responding to violations of the Policies and Procedures or agency procedures.

SOP#: CRR-006 Prepared by: CSP Effective date: 06/04

Title: ROLE: USER

Policy: All individuals at CSP and at the Participating Agency levels who require legitimate access to the software system will be granted such access.

Standard: Individuals with specific authorization can access the system software application for the purpose of conducting data management tasks associated with their area of responsibility.

Purpose: To outline the role and responsibilities of the system user.

Scope: System wide

Responsibilities:

CSP agrees to authorize use of the ServicePoint Software system only to users who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration or other essential activity associated with carrying out CSP's responsibilities.

The **Participating Agency** agrees to authorize use of the ServicePoint Software system only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

Users are any persons who use the ServicePoint software for data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the data security policy and standards as described in these Policies and Procedures. They are accountable for their actions and for any actions undertaken with their usernames and passwords.

SECTION 2:

Participation Requirements

SOP#: REQ-001 Prepared by: CSP Effective date: 06/04

Title: PARTICIPATION REQUIREMENTS

Policy: CSP staff will communicate requirements for participation. All requirements for participation are outlined in this document.

Standard: CSP staff and Participating Agencies will work to ensure that all sites receive the benefits of the system while complying with all stated policies.

Purpose: To provide the structure of on-site support and compliance expectations.

Scope: System wide

Procedure: Participation Agreement Requirements

- **High Speed Internet Connection Greater than or equal to 56k/v90:** DSL, Cable, etc.
- **Identification of Agency Administrator:** Designation of one key staff person to serve as Agency Administrator. This person will be responsible for creating usernames and passwords and monitoring software access. This person will also be responsible for training new staff persons on how to use the ServicePoint system.
- **Security Assessment:** Meeting of Agency Executive Director (or designee), Program Manager/Administrator and Agency Administrator with CSP staff member to assess and complete Agency Information Security Protocols. See attached Initial Implementation Requirements.
- **Training:** Commitment of Agency Administrator and designated staff persons to attend training(s) at CSP prior to accessing the system online. **Note**: Staff will **NOT** be allowed to attend training until **ALL** Information Security paperwork is complete and signed by Executive Director (or designee).
- **Interagency Data Sharing Agreements**: Interagency Data Sharing Agreements must be established between any shelter/service program where sharing of client level information is to take place. See attached Interagency Data Sharing Agreement.
- **Client Consent Forms** must be created for clients to authorize the sharing of their personal information electronically with other Participating Agencies through the ServicePoint software system where applicable. See attached Client Consent Form as an example.
- **Participation Agreement:** Agencies are required to sign a participation agreement stating their commitment to develop the policies and procedures for effective use of the system and proper collaboration with CSP Tech. See attached Initial Implementation Requirements.
- **Minimal Data Elements:** Agencies will be required to enter minimal data elements as defined by the CSP and its Steering Committee.

SOP #:REQ-002 Prepared by: CSP Effective date: 06/04

Title: IMPLEMENTATION REQUIREMENTS

Policy: All Participating Agencies must read and understand all participation requirements and complete all required documentation prior to implementation of the system.

Standard: All implementation requirements must be complete and on file prior to using the system.

Purpose: To indicate documentation requirements prior to implementation.

Scope: Participating Agencies

Procedure: CSP staff will assist Participating Agencies in the completion of all required documentation.

On Site Security Assessment Meeting: Meeting of Agency Executive Director or authorized designee, Program Manager/Administrator and Agency Administrator with CSP staff member to assist in completion of the Agencies' Information Security Protocols.

Participation Agreement
The Participation Agreement refers to the document agreement made between the participating agency and the CSP. This agreement includes commitment to minimal data as defined by the CSP and its Steering Committee on all clients. This document is the legally binding document that refers to all laws relating to privacy protections and information sharing of client specific information. See attached Initial Implementation Requirements.

Agency Participation/Data Sharing Agreements: Upon completion of the Security Assessment, each agency must agree to abide by all policies and procedures laid out in the CSP Security Manual. The Executive Director or designee will be responsible for signing this form. See attached Initial Implementation Requirements.

Identification of Referral Agencies: ServicePoint provides a resource directory component that tracks service referrals for clients. Each Participating Agency must compile a list of referral agencies and verify that the information has been entered into ResourcePoint.

SOP#: REQ-003 Prepared by: CSP Effective date: 06/04

Title: INTERAGENCY DATA SHARING AGREEMENTS

Policy: Data sharing among agencies will be supported upon completion of Interagency Sharing Agreements by Participating Agencies wishing to share client identified data.

Standard: For participating agencies to engage in data sharing arrangements, a written, formal document must be signed by the Executive Directors of each of the Participating Agencies involved in the data sharing.

Purpose: To explain the vehicle through which agencies can enter into an agreement allowing them to share client records.

Scope: Participating Agencies wishing to share client records.

Responsibilities:

Interagency Sharing Agreements

A. **Written Agreement**: Participating Agencies wishing to share information electronically through the ServicePoint System are required to provide, in writing, an agreement that has been signed between the Executive Directors of Participation Agencies. See attached Interagency Sharing Agreement.

B. **Role of Executive Director**: The Executive Director is responsible for abiding by all the policies stated in any Interagency Sharing Agreement.

Procedure:

A. Executive Directors wishing to participate in a data sharing agreement contact CSP staff to initiate the process.

B. Executive Directors complete the Interagency Sharing Agreement. Each participating agency retains a copy of the agreement and a master is filed with the CSP Organization.

C. Agency Administrators receive training on the technical configuration to allow data sharing.

D. Each Client whose record is being shared must agree via a written client consent form to have their data shared. A client must be informed what information is being shared and with whom it is being shared and for what length of time.

SOP#: REQ-004 Prepared by: CSP Effective date: 06/04

Title: WRITTEN CLIENT CONSENT PROCEDURE FOR ELECTRONIC DATA SHARING

Policy: As part of the implementation strategy of the system software, a Participating Agency must have client consent procedures and completed forms in place when electronic data sharing is to take place.

Standard: Client consent procedures must be on file prior to the assignment of user accounts to the site by CSP staff.

Purpose: To indicate the type of client consent procedures that Participating Agencies must implement prior to actual implementation.

Scope: Participating Agencies wishing to share client records

Procedure:

Client Consent Procedures

See attached Client Consent Form.

SOP#: REQ-005 Prepared by: CSP Effective date:06/04

Title: CONFIDENTIALITY AND INFORMED CONSENT

Policy: All Participating Agencies agree to abide by all privacy protection standards and agree to uphold all standards of privacy as established by CSP.

Standard: It is suggested that participating Agencies develop procedures for providing oral explanations to clients about the usage of a computerized Management Information System. Participating Agencies are required to use written client consent forms when information is to be shared with another agency.

Purpose: To ensure protection of clients' privacy.

Scope: Participating Agencies

Procedure:

Confidentiality/ Client Consent

Informed Consent: Oral Explanation (non-shared records): All clients should be provided an oral explanation that their information will be entered into a computerized record keeping system. The Participating Agency should provide an oral explanation of the CSP and the terms of consent. The agency may want to develop a fact sheet to post within the agency. CSP suggests including the following information in the fact sheet:

1. What ServicePoint is

Web based information system that services agencies across the county use to hold information about the persons that they serve.

2. Why the agency uses it

To understand their clients' needs help the programs plan to have appropriate resources for the people they serve to inform public policy

3. Security

Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records

4. Privacy Protection

No information will be released to another agency without written consent
Client has the right to not answer any question, unless entry into a program requires it
Client has the right to know who has added to, deleted, or edited their ServicePoint record
Information that is transferred over the web is through a secure connection

5. Benefits for clients

Case manager tells client what services are offered on site or by referral through the assessment process. Case manager and client can use information to assist clients in obtaining resources that will help them meet their needs.

6. Written Client Consent

Each Client whose record is being shared electronically with another Participating Agency must agree via a written client consent form to have their data shared. A client must be informed what information is being shared and with whom it is being shared.

7. **Information Release:** The Participating Agency agrees not to release client identifiable information to any other organization pursuant to federal and state law without proper client consent. See attached Client Consent Form.

8. **Federal/State Confidentiality Regulations**: The participating Agency will uphold Federal and State Confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.

    1) The Participating Agency will abide specifically by the Federal confidentiality rules as contained in 42 CFR Part 2 regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Participating Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
    2) The Participating Agency will abide specifically by State of Maryland general laws.

9. **Unnecessary Solicitation:** The Participating Agency will not solicit or input information from clients unless it is essential to provide services, or conduct evaluation or research.

SOP#: REQ-006 Prepared by: CSP Effective date: 06/04

Title: MINIMAL DATA ELEMENTS

Policy: Participating Agencies that collect client data through this Management Information system will, at a minimum, collect all data contained within the Profile Screen.

Standard: All agencies will collect minimal data elements.

Purpose: To ensure that agencies are collecting quality data.

Scope: Participating Agencies

Procedure:

Commitment to Utilization of Interview Protocol

Minimal Data Elements: The Participating Agency is responsible for ensuring that all clients are asked a minimal set of questions for use in aggregate analysis. These questions are contained within the Profile Screen.

SOP#: REQ-007 Prepared by: CSP Effective date: 06/04

Title: INFORMATION SECURITY PROTOCOLS

Policy: Participating Agencies must develop and have in place minimum information security protocols.

Standard: At a minimum, a Participating Agency must develop rules, protocols or procedures to address each of the following:

- Assignment of user accounts
- Unattended workstations
- Physical access to workstations
- Policy on user account sharing
- Client record disclosure
- Report generation, disclosure and storage

Purpose: To protect the confidentiality of the data and to ensure its integrity at the site.

Scope: Participating Agencies.

Procedures: To develop internal protocols, please reference Section 4.

SOP#: REQ-008 Prepared by: CSP Effective date: 06/04

Title: IMPLEMENTATION: CONNECTIVITY

Policy: Participating Agencies are required to obtain an adequate Internet connection (greater than or equal to 56K/v90)

Standard: Any Internet connection greater than or equal to 56K/v90 is acceptable.

Purpose: To ensure proper response time and efficient system operation of the Internet application.

Scope: Participating Agencies

Procedure: CSP staff is committed to informing all participating agencies about availability of Internet providers. Obtaining and maintaining an Internet connection greater than or equal to 56K/v90 is the responsibility of the participating agency.

SOP#: REQ-009 Prepared by: CSP Effective date: 06/04

Title: MAINTENANCE OF ONSITE COMPUTER EQUIPMENT

Policy: Participating Agencies commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation.

Standard: Participating Agencies must meet the technical standards for minimum computer equipment configuration, Internet connectivity, data storage and data back up.

Purpose: To ensure that participating agencies adopt an equipment and data maintenance program.

Scope: Participating Agencies

Responsibilities:

The Executive Director or designee will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the CSP including the following:

A. **Computer Equipment:** The Participating Agency is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in the CSP.

B. **Backup**: The Participating Agency is responsible for supporting a backup procedure for each computer connecting to the CSP.

C. **Internet Connection**: CSP staff members are not responsible for troubleshooting problems with Internet Connections.

D. **Virus Protection**: As a matter of course, each agency should install virus protection software on all computers.

E. **Data Storage**: The Participating Agency agrees to only download and store data in a secure format.

F**. Data Disposal**: The Participating Agency agrees to dispose of documents that contain identifiable client level data by shredding paper records, deleting any information from diskette before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal of property. CSP staff are available to consult on appropriate processes for disposal of electronic client level data.

SECTION 3:

Training

SOP#: TRA-001 Prepared by: CSP Effective date: 06/04

Title: TRAINING SCHEDULE

Policy: CSP staff will maintain an ongoing training schedule to adequately meet the needs of Participating Agencies.

Standard: CSP staff will publish a schedule for trainings and will offer them regularly.

Purpose: To provide ongoing training to participating agencies.

Scope: System wide

Procedure: A training schedule will be sent via email each month. Agencies are asked to RSVP for all trainings. Training sessions will be offered at Carroll County Government Building unless otherwise noted.

SOP#: TRA-002 Prepared by: CSP Effective date: 06/04

Title: USER, ADMINISTRATOR AND SECURITY TRAINING

Policy: All users must undergo security training before gaining access to the system. This training must include a review of CSP's security Policies and Procedures.

Standard: CSP staff or trained Agency Administrator will provide data security training

Purpose: To ensure that staff are properly trained and knowledgeable of CSP's security Policies and Procedures.

Scope: System wide

Procedure: Agency staff must attend user training. Agency Administrators must also attend an Administrator training in addition to user training. Agencies will be notified of scheduled training sessions.

Training: The Agency Administrator is responsible for training new users. Users must receive ServicePoint training prior to being granted user privileges for the system.

SECTION 4:

User, Location, Physical and Data Access

SOP#: ACC-001 Prepared by: CSP Effective date: 06/04

Title: ACCESS PRIVILEGES TO SYSTEM SOFTWARE

Policy: Participating Agencies will apply the user access privilege conventions set forth in this procedure.

Standard: Allocation of user access accounts and privileges will be made according to the format specified in this procedure.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

User Access Privileges to ServicePoint

A. User access: User access and user access levels will be deemed by the Executive Director of the Participating Agency in consultation with the Agency Administrator. The Agency Administrator will generate username and passwords within the Administrative function of ServicePoint.

B. User name format: The Agency Administrator will create all usernames using the First Initial of First Name and Last Name. Example John Doe's username would be JDoe. In the case where there are two people with the same first initial and last name, a sequential number should be placed at the end of the above format. Ex. JDoe2, JDoe3.

C. Passwords:

1. **Creation:** Passwords are automatically generated from the system when a user is created. Agency Administrators will communicate the system-generated password to the user.
2. **Use of:** The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and contain 2 numbers.
3. **Expiration:** Passwords expire every 45 days.
4. **Termination or Extended Leave from Employment:** The Agency Administrator should terminate the rights of a user immediately upon termination from their current position. If a staff person is to go on leave for a period of longer than 45 days, their password should be inactivated within 5 business days of the start of their leave. The Agency Administrator is responsible for removing users from the system. The Agency Administrator must update the access list and signed agreement on a quarterly basis.

SOP#: ACC-002 Prepared by: CSP Effective date: 06/04

Title: ACCESS LEVELS FOR SYSTEM USERS

Policy: Participating Agencies will manage the proper designation of user accounts and will monitor account usage.

Standard: The Participating Agency agrees to apply the proper designation of user accounts and manage the use of these accounts by agency staff.

Purpose: To enforce information security protocols

Scope: Participating Agencies

Procedure: User accounts will be created and deleted by the Agency Administrator under authorization of the Participating Agency's Executive Director.

User Levels: There are 9 levels of access to the ServicePoint system. These levels should be reflective of the access a user has to client level paper records. and access levels should be need-based. Need exists only for those staff, volunteers, or designated personnel who work with (or supervise staff who work directly with) clients or have data entry responsibilities. A Matrix describing the access levels is included in this packet.

SOP#: ACC-003 Prepared by: CSP Effective date: 06/04

Title: LOCATION ACCESS PRIVILEGES TO SYSTEM SERVER

Policy: Participating Agencies agree to enforce the location access privileges to the system server.

Standard: Only authorized computers will be able to access the system from authorized locations.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

Location Access: Access to the system software system will only be allowed from computers specifically identified by the Executive Director and Agency Administrator of the Participating Agency. Those designated computers will be registered electronically with the Central Server by CSP staff. Laptops and off-site installations will require an additional security form stating that use will not be for unauthorized purposes from unauthorized locations. See attached Laptop and Off-Site Installation Access Privileges to System Server Commitment Form.

SOP#: ACC-004 Prepared by: CSP Effective date: 06/04

Title: ACCESS TO DATA

Policy: Participating Agencies must agree to enforce the user access privileges to system data server as stated below.

Standard:

A. User Access: Users will only be able to view the data entered by users of their own agency. Security measures exist within the ServicePoint software system which restricts agencies from viewing each other's data.

B. Raw Data: Users who have been granted access to the ServicePoint Report Writer tool have the ability to download and save client level data onto their local computer. Once this information has been downloaded from the ServicePoint server in raw format to a agency's computer, these data then become the responsibility of the agency. A participating Agency should develop protocol regarding the handling of data downloaded from the Report Writer.

C. Agency Policies Restricting Access to Data: The Participating Agencies must establish internal access to data protocols. These policies should include who has access, for what purpose, and how they can transmit this information. Issues to be addressed include storage, transmission and disposal of these data.

D. Access to Countywide ServicePoint Data: Access will be granted based upon policies developed by the Access to Data Subcommittee of the Steering Committee.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

SOP#: ACC-005 Prepared by: CSP Effective date: 06/04

Title: ACCESS TO CLIENT PAPER RECORDS

Policy: Participating Agencies will establish procedures to handle access to client paper records.

Standard: The Participating Agencies agree to establish procedures regarding how staff has access to client paper records.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

- Agencies need to have a policy regarding access to client paper records.
- Identify how and where client paper records are stored.
- Develop policy regarding length of storage and disposal procedure of paper records.
- Develop policy on disclosure of information contained in client paper records.

SOP#: ACC-006 Prepared by: CSP Effective date: 06/04

Title: PHYSICAL ACCESS CONTROL

Policy: Physical access to the system data processing areas, equipment and media must be controlled. Access must be controlled for the transportation of data processing media and other computing resources. The level of control is contingent on the level of risk and exposure to loss.

Standard: Personal computers, software, documentation and diskettes shall be secured proportionate with the threat and exposure to loss. Available precautions may include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.

Purpose: To delineate standards for physical access.

Scope: System wide

Guidelines:

Access to computing facilities and equipment

- The CSP staff with the Agency Administrators within Participating Agencies will determine the physical access controls appropriate for their organizational setting based on CSP security policies, standards and guidelines.
- All those granted access to an area or to data are responsible for their actions. Additionally, those granting another person access to an area are responsible for that person's activities.

Media and hardcopy protection and transportation

- Printed versions of confidential data should not be copied or left unattended and open to unauthorized access.
- Media containing client-identified data will not be shared with any agency other than the owner of the data for any reason. CSP data may be transported by authorized employees using methods deemed appropriate by the participating agency that meet the above standard. Reasonable care should be used, and media should be secured when left unattended.
- Magnetic media containing CSP data which is released and/or disposed of from the Participating Agency and Central Server should first be processed to destroy any data residing on that media.
- Degaussing and overwriting are acceptable methods of destroying data.
- Responsible personnel must authorize the shipping and receiving of magnetic media, and appropriate records must be maintained.
- CSP information in hardcopy format should be disposed of properly.

SOP#: ACC-007 Prepared by: CSP Effective date: 06/04

Title: UNIQUE USER ID AND PASSWORD

Policy: Authorized users will be granted a unique user ID and password.

Standard:

- Each user will be required to enter a User ID with a Password in order to logon to the system.
- User ID and Passwords are to be assigned to individuals.
- The User ID will be the first initial and full last name of the user. If a user has a first initial and last name that is identical to a user already in the system, the User ID will be the first initial and last name plus the number 01.
- The Password must be no less than eight and no more than sixteen characters in length.
- The password must be alphanumeric with a minimum of two numeric.

Purpose: In order to ensure that only authorized users will be able to enter, modify or read data, unique User ID will be issued to every user.

Scope: System wide

Procedures:

- Discretionary Password Reset Initially each user will be given a password for one time use only. The first or reset password will be automatically generated by ServicePoint and will be issued to the User by the Agency Administrator. Passwords will be communicated in written or verbal form. The first time, temporary password can be communicated via email. CSP staff is not available to agency staff to reset passwords. Only an Agency Administrator can reset a password.
- Forced Password Change (FPC) FPC will occur every forty-five days once a user account is issued. Passwords will expire and users will be prompted to enter a new password. Users may not use the same password consecutively, but may use the same password more than once.
- Unsuccessful logon if a User unsuccessfully attempts to logon three times, the User ID will be “locked out”, access permission revoked and unable to gain access until their account is reset.

SOP#: ACC-008 Prepared by: CSP Effective date: 06/04

Title: RIGHT TO DENY USER AND PARTICIPATING AGENCY'S ACCESS

Policy: Participating Agency or a user access may be suspended or revoked for suspected or actual violation of the security protocols.

Standard: Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access.

Purpose: To outline consequences for failing to adhere to information security protocols.

Scope: Participating Agency

Procedure:

1. All potential violations of any security protocols will be investigated.
2. Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions from CSP may include; additional training, suspension of user license to loss of user license.
3. Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
4. All sanctions are imposed by the CSP Governing Body.

SOP#: ACC-009 Prepared by: CSP Effective date: 06/04

Title: DATA ACCESS CONTROL

Policy: Agency Administrators at Participating Agencies and CSP staff must monitor access to system software.

Standards: Agency Administrators at Participating Agencies and CSP staff must regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access.

Agency Administrators at Participating Agencies and CSP staff must implement discretionary access controls to limit access to CSP information when available and technically feasible.

Participating Agencies and CSP staff must audit all unauthorized accesses and attempts to access CSP information. Audit records shall be kept at least six months, and Agency Administrators and CSP staff will regularly review the audit records for evidence of violations or system misuse.

Purpose: To indicate the standards and guidelines for data access control for the participating agency.

Scope: System wide

Guidelines:

- Access to computer terminals within restricted areas should be controlled through a password or through physical security measures.
- Each user should have a unique identification code.
- Each user's identity should be authenticated through an acceptable verification process.
- Passwords are the individual's responsibility, and users cannot share passwords.
- Users should be able to select and change their own passwords, and must do so at least every forty-five days. A password cannot be re-used until 2 password selections have expired.
- Passwords should not be able to be easily guessed or found in a dictionary. The password format is alphanumeric.
- Any passwords written down should be securely stored and inaccessible to other persons. Users should **not** store passwords on a personal computer for easier log on.

SOP#: ACC-010 Prepared by: CSP Effective date: 06/04

Title: AUDITING: MONITORING, VIOLATIONS AND EXCEPTIONS

Policy: CSP staff will monitor access to all systems that could potentially reveal a violation of information security protocols.

Standard: **Monitoring**
CSP staff will monitor compliance with the data security standards.

Violations
Any exception to the data security policies and standards not approved by CSP is a violation, and will be reviewed for appropriate disciplinary action that could include termination of employment or criminal prosecution.

Exceptions
All exceptions to these standards are to be requested in writing by the Executive Director of the Participating Agency and approved by CSP Steering Committee as well as CSP's Management Team.

Purpose: To outline the standards and procedures on compliance with information security protocols and the process by which CSP staff will monitor compliance with such policies.

Scope: System wide

Monitoring
- Monitoring compliance is the responsibility of CSP.
- All users and custodians are obligated to report suspected instances of noncompliance.

Violations
- CSP staff will review standards violations and recommend corrective and disciplinary actions.
- Users should report security violations to the Agency Administrator, or CSP staff person as appropriate.

Exceptions
- Any authorized exception to this policy must be issued from CSP's Management Team and the Participating Agency's Executive Director.

SOP#: ACC-011 Prepared by: CSP Effective date: 06/04

Title: LOCAL DATA STORAGE

Policy: Client records containing identifying information that are stored within the Participating Agency's local computers are the responsibility of the Participating Agency.

Standard: Participating Agencies should develop policies for the manipulation, custody and transmission of client-identified data sets.

Purpose: To delineate the responsibility that Participating Agencies have for client-identified data.

Scope: Participating Agencies

Procedure: A Participating Agency develops policies consistent with Information Security Policies outlined in this document regarding client-identifying information stored on local computers.

SOP#: ACC-012 Revision: Prepared by: CSP Effective date: 06/04

Title: TRANSMISSION OF CLIENT LEVEL DATA

Policy: Client data will be transmitted in such a way as to protect client privacy and confidentiality.

Standards: Administrators of the Central Server data must be aware of access-control vulnerabilities for that data while they are in transmission within the network.

Purpose: To provide guidelines regarding security of client level data during transmission.

Scope: System wide

Guidelines: Transmission will be secured by 128-bit encryption provided by SSL Certificate protection, which is loaded at the CSP server.

SECTION 5:

Technical Support and System Availability

SOP#: SUP-001 Prepared by: CSP Effective date: 06/04

Title: PLANNED TECHNICAL SUPPORT

Policy: CSP staff will offer a standard technical support package to all Participating Agencies.

Standard: CSP staff will provide technical assistance to Participating Agencies on use of the system software.

Purpose: To describe the elements of the technical support package offered by CSP staff.

Scope: System wide

Procedure: CSP staff will assist agencies in:

- Start-up and implementation
- On-going technical assistance
- Training
- Technical assistance with report writing

SOP#: SUP-002 Prepared by: CSP Effective date: 06/04

Title: Participating Agency Service Request

Policy: CSP staff will respond to requests for services that arrive from the Agency's Executive Director or the Agency Administrator

Standard: To effectively respond to service requests, CSP Staff will require that proper communication channels be established and used at all times.

Purpose: To outline the proper methods of communicating a service request from a Participating Agency to a CSP Staff member.

Scope: Participating Agencies.

Procedure:

Service Request from Participating Agency

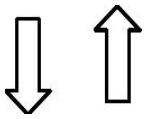
1. Agency Management (Exec. Director or Agency Administrator) contact CSP staff for service.

2. CSP Staff member assigned to Agency determines resources needed for service.

3. CSP contacts agency management staff to work out a mutually convenient schedule.

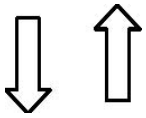
Chain of Communication

Agency Staff



Agency Management Staff

Executive Director or Agency Administrator



CSP Staff

SOP#: SUP-003 Prepared by: CSP Effective date: 06/04

Title: AVAILABILITY: HOURS OF SYSTEM OPERATION

Policy: The system will be available to the community of users in a manner consistent with the user's reasonable usage requirements.

Standard: Members of the CSP staff via Bowman agree to minimally operate the system web site twenty four hours a day/ seven days a week. Some time may be required each day to backup the server and database.

Purpose: To communicate that the system must be down to maintain the servers and the databases. Bowman Internet Systems is in complete control of scheduled outages.

Scope: System wide

Schedule: The system will be available 24 hours a day, seven days a week, excluding maintenance, acts of god, or federal or state declared emergency situations.

SOP#: SUP-004 Prepared by: CSP Effective date: 06/04

Title: AVAILABILITY: CSP STAFF AVAILABILITY

Policy: CSP staff will be available to the community of users in a manner consistent with the user's reasonable service request requirements.

Standard: CSP staff is generally available for Technical Assistance, questions, and troubleshooting between the hours of 8:30 and 12:30 Monday to Friday, any exceptions to this availability will be posted on the System Bulletin Board Area in ServicePoint.

Purpose: To when CSP staff will be available to resolve technical issues.

Scope: System wide

Procedure: SOP#: SUP-005 Prepared by: CSP Effective date: 06/04

Title: AVAILABILITY: PLANNED INTERRUPTION TO SERVICE

Policy: CSP staff will inform Participating Agencies of any planned interruption to service.

Standard: Participating Agencies will be notified of planned interruption to service one week prior to the interruption.

Purpose: To indicate procedures for communicating interruption to service. To indicate procedures for communicating when services resume.

Scope: System-wide

Procedure:

Planned Interruption to Service

CSP staff will notify Participating Agencies via e-mail and/or fax the schedule for the interruption to service. An explanation of the need for the interruption will be provided and expected benefits or consequences articulated.

Service Restoration

Unless the original communication stated the resumption time CSP staff will notify via e-mail and/or fax that service has resumed.

SOP#: SUP-006 Prepared by: CSP Effective date: 06/04

Title: AVAILABILITY: UNPLANNED INTERRUPTION TO SERVICE

Policy: Participating Agencies may or may not be notified in advance of unplanned interruption to service.
Standard: Participating Agencies will be notified of unforeseen interruption to service that are expected to exceed two hours.
Purpose: To indicate procedures for communicating unforeseen interruption to service.
Scope: System wide

Unplanned Interruption to Service

When an event occurs that makes the system inaccessible Bowman staff will make every effort to get the system back up. CSP staff will notify via e-mail and/or fax that service has resumed.

SECTION 6:

Data Release Protocols

SOP#: DAT-001 Prepared by: CSP Effective date: 06/04

Title: DATA RELEASE AUTHORIZATION AND DISTRIBUTION

Policy: CSP staff will follow Steering Committee procedures for the release of all data.

Standard: CSP staff will abide by Carroll County Access to Data Policies as well as those established by the Steering Committee.

Purpose: To outline the procedures for the release of data from the CSP.

Scope: Steering Committee and CSP staff.

Procedure: All data that are to be released in aggregate format must represent at least sixty percent (60%) of the clients in that region.

Release of data principals (Participating Agency)

- Only de-identified aggregate data will be released.
- Program specific information will not be released without the written consent of the Participating Agency Executive Director.
- There will be full access to aggregate data for all participating agencies.
- Aggregate data will be available in the form of an aggregate report or as a raw data set.
- Aggregate data will be made directly available to the public in the future.
- Parameters of the aggregate data, that is, where the data comes from, what it includes and what it does not include will be presented with each report.
- An executive committee shall be put in place when approval is required for release of data that do not meet the 60% release rate.

SOP#: DAT-002 Prepared by: CSP Effective date: 06/04

Title: RIGHT TO DENY ACCESS TO CLIENT IDENTIFIED INFORMATION

Policy: CSP retains authority to deny access to all client identified information contained within the system.

Standard: No data will be released to any person, agency, or organization that is not the owner of said data.

Purpose: To protect client confidentiality

Scope: System wide

Procedure:

1. Any request for client identified data from any person, agency, or organization other than the owner will be forwarded to the CSP Management for review.
2. Pursuant to CSP Management any outside entity must obtain the written consent of every client contained within the database prior to the release of the data.

SOP#: DAT-003 Prepared by: CSP Effective date: 06/04

Title: RIGHT TO DENY ACCESS TO AGGREGATE INFORMATION

Policy:	CSP staff retains authority to deny access to all aggregate data contained within the system.
Standard:	No data will be released without proper authorization
Purpose:	To prevent the unauthorized distribution of aggregated reports.
Scope:	System wide
Procedure:	When a person or organization requests data, the request will be reviewed the CSP staff.

.

ATTACHMENTS

User Access Agreement

This contractual agreement is entered into on _____between the **CSP** and

Agency Name: _____

Executive Director: _____

Name of person completing agreement: _____

Address: _____ Phone: (____)_____-_____
_____ Fax: (____)_____-_____
_____ Email:
_____

This document contains the specific obligations that each agency must follow in order to participate in the CSP. The signatory for this document shall be the Agency Executive Director or designee.

I. Contractual Requirements and Roles

_____
Signature

I agree to abide by the following policies as contained in **Section 1** of the CSP Policies and Procedures as described below.

A. **Steering Committee:** Advises the project on all activities.
B. **Participating Agency Executive Director**: Assumes responsibility for the entire implementation and administration of the system
C. **Participating Agency Agency Administrator**: The Executive Director's officially designated Representative to manage ServicePoint operations.
D. **Participating Agency User**: Agency Staff who serve clients who are authorized by the Executive Director to access the system.

II. Participation Requirements

_____
Signature

I agree to abide by the following policies as contained in **Section 2** of the CSP Policies and Procedures.

A. **Participation Requirements of Participating Agency and CSP:** Lays out responsibilities of all parties involved in implementation.
B. **Implementation Documentation:** Delineates all written documentation required for implementation including data sharing agreements, client consent forms, data collection commitment and participating agency security protocols.
C. **Minimal Data Elements**: Participating agencies must make every effort to enter information on all clients served in participating programs. Agencies agree to

enter at a minimum, all data contained within the Profile Screen.

D. **Confidentiality**: The Participating Agency will uphold Federal and State Confidentiality regulations that protect client records and privacy as referenced in 42 CFR Part 2, Health Insurance Portability and Accountability Act (HIPAA) and Maryland general law.
E. **Maintenance of Internet Connection and Onsite Computer Equipment:** Outlines responsibility of agency in maintaining connectivity and equipment.

III. Training

_____
Signature

I agree to abide by the following policies as contained in **Section 3** of the CSP Policies and Procedures as described below.

A. **Training Schedule**: CSP staff will provide schedule and on site training as documented.
B. **User, Administration and Security Training**: Prior to being granted access to the system, all staff will be trained on relevant information security issues.

IV. User, Location, Physical, and Data Access

_____
Signature

I agree to abide by the following policies as contained in **Section 4** of the CSP Policies and Procedures as described below.

A. **User Access**: Identifies process for user access including authorization of user names and passwords
B. **Location Access**: Participating agencies must identify the locations from which system software can be accessed.
C. **Physical Access**: All agencies must develop internal access policies to all systems.
D. **Data Storage and Transmission**: All agencies will develop internal protocols for the transmission and storage of client level information. CSP staff is available to provide recommendations for policy development.

V. Technical Support and System Availability

_____
Signature

I agree to abide by the following policies as contained in **Section 5** of the CSP Policies and Procedures as described below.

A. **Planned Technical Support:** Participating agencies will receive planned technical support as requested.
B. **Availability:** System software will be made available for set periods of time with time allowed for updates and protocols for unplanned interruption to service.

VI. Data Release Protocols

_____
Signature

I agree to abide by the following policies as contained in **Section 6** of the CSP Policies and Procedures as described below.

A. **Data Release Authorization:** Outlines specific policies regarding release of aggregate data.

By signing this document, I agree to abide by all policies as stated in the CSP Policies and Procedures Document. I also agree to educate all staff members in my agency as to the policies that directly affect their work.

Name of Program	Title of Person Completing Agreement	
Name of Sponsoring Agency	Signature of Person Completing Agreement	Date
Executive Director	Signature of Executive Director	Date
CSP Staff Person	Signature of CSP Staff Person	Date

CSP (Community Service Point)

Program Information

Please complete for each program in the agency which will be linking data to ServicePoint.

Agency Name: _____

Program Name: _____

Date: _____

Address: _____

City: _____ **State:** **Zip:** _____

Completed by: _____ **Phone Number:** _____

Type of Program: (circle)	Emergency Shelter Transitional Housing Permanent Supportive Housing Supportive Services Only Outreach Other: specify _____			
Population Served:	Individuals	Families	Both	(circle all that apply)

Target Population (ex. Youth, Elders): _____

Please describe services offered at your agency:

Please describe your agency's capacity, for example with Shelters describe with respect to number of rooms and descriptions of beds within rooms. Note Floor level if more than one floor.

Community ServicePoint User Access Set-up Form

Program Name: _____ Date: _____

Agency Administrator: _____Executive Director: _____

Staff Name	Access Level (see below)	Status (active/inactive)	Authorized By	Date
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				

	Resource Specialist I	Resource Specialist II	Resource Specialist III	Volunteer	Agency Staff	Case Manager	Agency Admin.	Executive Director	SA I	SA II
ClientPoint										
Profile				X	X	X	X	X	X	X
Employment						X	X	X	X	X
Residential Hist.						X	X	X	X	X
Medical/Addict.							X	X	X	X
Legal						X	X	X	X	X
Military						X	X	X	X	X
Case Notes						X	X	X	X	X
Worksheets					X	X	X	X	X	X
ServicePoint										
Referrals				X	X	X	X	X	X	X
Check-in/out				X	X	X	X	X	X	X
Other services					X	X	X	X	X	X
ResourcePoint	X	X	X	X	X	X	X	X	X	X
ShelterPoint				X	X	X	X	X	X	X
Reports						X	X	X	X	X
Administration										
Add Users							X	X	X	X
Remove Users							X	X	X	X
Reset Password							X	X	X	X
Add Agency									X	X
Edit Agency		X	X				X	X	X	X
Remove Agency									X	X
Picklist options									X	X
Licenses									X	X
Other options									X	X

Location Access Authorization

Please list the locations and users of each computer that should be registered with the CSP server that can access the ServicePoint software system.

Location	Computer Description	Users of Computer	Registered with Server (CSP staff only)

CSP (Community Service Point)

Laptop and Off Site Installation Access Privileges to System Server Commitment Form

Security Agreement

This agreement is made between the CSP and _____.
Agency Name

By signing this security agreement, I agree that I will not allow persons other than Agency authorized staff to use the laptop. I understand that I will only access the ServicePoint software from locations authorized by the agency as appropriate for entering data. I realize that if I access the ServicePoint software from an unauthorized agency location that I am putting the confidentiality of all of the clients served in this agency at risk.

By signing this document, I agree to abide by the above policies.

_____ _____
Staff name Date

_____ _____
Agency name Date

Interagency Data Sharing Agreement

The CSP administers a computerized record keeping system that captures information about people experiencing homelessness and other service needs. The system, ServicePoint, allows programs the ability to share information electronically about clients who have been entered into the software. Client level information can only be shared between agencies that have established an Interagency Sharing Agreement and have received written consent from particular clients agreeing to share their personal information with another agency.

The agency receiving the written consent has the ability to "share" that client's information electronically through the ServicePoint system with a collaborating agency.

This process can benefit clients by eliminating duplicate intakes. Intake and exit interviews can be shared, with written consent, between

_____

NAMES OF COLLABORATING AGENCIES.

By establishing this agreement, the

_____

NAMES OF COLLABORATING AGENCIES

agree that within the confines of the CSP and ServicePoint software:

1) ServicePoint information in either paper or electronic form will never be shared outside of the originating agency without client written consent.
2) Client level information will only be shared electronically through the ServicePoint System with agencies the client has authorized to see their information.
3) Information that is shared with written consent will not be used to harm or deny any services to an eligible client.
4) A violation of the above will result in immediate disciplinary action.
5) Client owned Information will be deleted from the system upon client request.
6) Clients have the right to request information about who has viewed or updated their ServicePoint record.

We at _____

NAMES OF COLLABORATING AGENCIES.

establish this interagency sharing agreement so that our agencies will have the ability to share client level information electronically through the ServicePoint System. This agreement does not pertain to client level information that has not been entered into the ServicePoint system. This electronic sharing capability only provides us with a tool to share client level information. This tool will only be used when a client provides written consent to have his/her information shared.

NAMES OF COLLABORATING AGENCIES

also have an agreement with the CSP and have completed security procedures regarding the protection and sharing of client data.
By signing this form, on behalf of our agencies, I authorize the CSP to allow us to share information between our agencies. We agree to follow all of the above policies to share information between our collaborating agencies.

We agree the share the following information (please check all that apply):

- Basic Client Profile Information
- Required Data Elements (HUD Universal Data Elements)
- Children's Required Data Assessment (HUD Required Data Elements for Children)
- HUD 40118 Assessment (HUD APR fields
- Other (Please Specify)

Agency 1	Agency 2
Printed Name of Executive Director	Printed Name of Executive Director
Signature of Executive Director	Signature of Executive Director
Date	Date

SAMPLE Client Consent Form

The CSP administers a computerized record keeping system that captures information about people experiencing homelessness, including their service needs. The programs in the **AGENCY NAME** have decided to use CSP as their data management tool to collect information on the clients they serve and the services they provide.

This process benefits you because will not have to complete an additional intake interview. Intake information can be shared, with your written consent, from your service program to the **COLLABORATING AGENCY**.

If you consent, we have the ability to share your intake information with the **COLLABORATING AGENCY** to be used for an initial intake assessment. You can choose to share all or part of the information that you have shared including basic demographic information, residential, employment skills/income, military/legal, service needs, goals and outcomes. Your information will be shared electronically via a secure, encrypted, web-based system to the agencies of your choice. This will not take place unless you provide written consent. No medical, mental health, or substance use history will be shared unless you provide express written consent below. Your record will be shared for a period of no greater than five years from today's date.

The information that you share with the **COLLABORATING AGENCY** will be used to help you access services that will help you obtain and maintain permanent housing. You can choose to have any information that you have shared deleted from the system at any time as well as request a document containing information about who has viewed or updated your ServicePoint record. The information that you provide, combined with that provided by others, will be used, without any identifying information, for reporting requirements and advocacy.

We here at **AGENCY NAME** have an interagency sharing agreement with the **COLLABORATING AGENCY** regarding clients that are served by both agencies. Both programs also have an agreement with the CSP and have completed security procedures regarding the protection and sharing of client data.

I, _____ _____ ☐ CONSENT

(Participant Signature) (Date) ☐ DO NOT CONSENT

to have information (demographic, residential, employment, income, military, legal, services, and goals and outcomes) that I provided in intake interviews to staff at **AGENCY NAME** to be shared electronically with the **COLLABORATING AGENCY** using the CSP Computerized Record Keeping System.

MEDICAL, MENTAL HEALTH and SUBSTANCE USE HISTORY SHARING AUTHORIZATION

I, _____ _____ ☐ CONSENT

(Participant Signature) (Date) ☐ DO NOT CONSENT

to have information (medical, mental health, and substance use history) that I provided in intake interviews to staff at **AGENCY NAME** to be shared electronically with the **COLLABORATING AGENCY** using the CSP Computerized Record Keeping System. Agencies are responsible for being aware of HIPAA compliance when sharing.
I understand that I may ask to have this information removed from the CSP computerized record keeping system at any time in the future.

(Participant Signature)	Date
(Staff MemberSignature)	Date

CSP (Community Service Point)

Referral Agencies

Please provide the top referral agencies/program (including services provided) utilized each agency program for inclusion in ResourcePoint, the service directory component of ServicePoint. You will be contacted for verification of information prior to entry into ResourcePoint.

Agency	Program	Phone number	Services Provided