PromisSE Policies and Procedures

For FL-505

Lead Agency: Okaloosa Walton Homeless Continuum of Care

Program Management Information Systems of the Southeast (PromisSE)

Homeless Management Information System (HMIS)

Operating Policy and Procedure

The purpose of the HMIS is to record and store client-level information about the numbers, characteristics and needs of persons who use homeless housing and supportive services, to produce an unduplicated count of homeless persons for each Continuum of Care; to understand the extent and nature of homelessness locally, regionally and nationally; and to understand patterns of service usage and measure the effectiveness of programs and systems of care. The following operating policies and procedures apply to all designated HMIS participating Agencies (Contributing HMIS Organizations – CHOs).

PRIVACY STATEMENT

Okaloosa Walton Homeless Continuum of Care, hereinafter referred to as the PromisSE's HMIS Lead Agency for Okaloosa and Walton Counties, is committed to making the HMIS safe for all types of programs in the PromisSE service area, the clients whose information is recorded, and to maximize the opportunities to improve services through automation.

Toward that end:

- Sharing is a planned activity guided by Participation Agreements between Continuum Designated HMIS Lead Agencies. The Continuum Designated HMIS Lead Agency may elect to keep private some or all of the client record, including all identifying data.
- All organizations will screen for safety issues related to the use of the automation.
- PromisSE's HMIS Lead Agency has systematized the risk assessment related to clients through the PromisSE Release, offered options in terms of the SS#, and in the Privacy Notice is explained.
- PromisSE's HMIS Lead Agency has adopted a Privacy Notice that was developed in close collaboration with those providers that manage information that may put a client at risk.
- PromisSE's HMIS Lead Agency System runs in compliance with HIPAA, and all Federal and State laws and codes. All privacy procedures are designed to ensure that the broadest range of providers may participate in the Project.

  Privacy Training is a requirement for all Agencies and End Users on the System.
- We view our Privacy Training as an opportunity for all participating organizations to revisit and improve their overall privacy practice.

- All those issued user access to the System must successfully complete HMIS training, which includes a privacy training module. End Users must also sign a User's Agreement, as well as a PromisSE HMIS Agency Participation Agreement. Taken together, these documents obligate participants to core privacy procedures. If Agencies decide to share information outside PromisSE, they must sign an agreement that defines sharing practice and prevents re-release of information.
- Policies have been developed that protect not only client's privacy, but also Agency's privacy. Practice Principles around the use and publication of Agency or Continuum designated HMIS Lead Agency specific data have been developed and included in both the Participation Agreement and the Policies and Procedures.
- The HMIS System allows programs with multiple components/locations that serve the same client to operate on the a single case plan, reducing the amount of staff and client's time spent in documentation activities and ensuring that care is coordinated and messages to clients are reinforced and consistent.

Key Terms and Acronyms:

Term	Acronym (if used)	Brief Definition
Homeless Management Information System	HMIS	Data systems that meet HUD requirements and are used throughout the nation to measure homelessness and the effectiveness of related service delivery systems. The HMIS is also the primary reporting tool for HUD homeless service grants as well as other public monies related to homelessness.
Continuum of Care	CoC	Planning body charged with guiding the local response to homelessness.
Balance of State CoCs	BOS	Areas that make up the "Balance of State".
Contributing HMIS Organizations	CHO	An organization that participates on the HMIS.

Participation Agreement		The Agreement between all participating Continuum Designated HMIS Lead Agencies and PromisSE's HMIS Lead Agency that specifies the rights and responsibilities of PromisSE's HMIS Lead Agency and participating Continuum Designated HMIS Lead Agencies. This document also outlines privacy, inter-Agency sharing, custody of data, data entry standards, and reporting standards. The Agreement prevents the re-release of data and, in combination with the PromisSE License Agreement, defines the rules of sharing. The Agreement between each Continuum Designated HMIS Lead Agency and PromisSE's HMIS Lead Agency that supports a regional HMIS operating in a single system environment.
PromisSE License Agreement		The Agreement signed by each end user and Agency manager that outlines guidelines for use including; individual privacy, Agency privacy and other PromisSE policy and procedure for use of the HMIS system. This document sets the standards of conduct for each HMIS user.
Release of Information	ROI	An electronic ROI must be completed to share or enter any person's data within the HMIS system.
Visibility		Refers to the ability to see a client's data between provider pages on the HMIS. Visibility is configured on the HMIS system in each Provider Page.
Visibility Groups		Visibility Groups are defined groups of Provider Pages where data is shared. Internal Visibility Groups control internal sharing.

Coverage Rate		For Continuum Designated HMIS Lead Agency - The percent of the Homeless Population that is measured on HMIS. Coverage estimates are used to project to a total homeless count that includes those served in Domestic Violence Providers or other non-participating Shelters or Outreach Programs. See HUD's Coverage Memo for guidance. HUD also defines Bed Coverage (beds covered on the HMIS) and Service Coverage (person coverage for non- residential programs).

Program Types		HUD defines 9 basic Program Types ● ES: Emergency Shelter- Overnight shelters or shelters with a planned length of stay of less than 3 months. ● TH: Transitional Housing- Transitional environments that have a planned LOS of not more than 2 years and provide supportive services. ● PSH: Permanent Supportive Housing- Permanent Housing for the formerly homeless with services attached to persons served under this program. ● PH: Permanent Housing- Permanent housing that may be supported by a voucher but does not have services attached to the housing. ● RRH: Rapid Rehousing- A program that rapidly rehouses those that are identified as Literally Homeless. ● HP: Homeless Prevention- A program that helps persons at imminent risk of losing housing, to retain their housing. ● SOP: Street Outreach Program- A program that serves homeless persons who are living on the street or other places not meant for habitation. ● SSO: Services Only Program- A program that serves only with no residential component. These programs often provide case management and other forms of support and meet with clients in an office, at the household's home, or in a shelter. ● Safe Haven: A program that provides low-demand shelter for hard-to-serve persons with severe disabilities. The clients have often failed in other sheltering environments.
Length of Stay	LOS	The number of days between the beginning of services and the end of services. It is calculated using entry and exit dates or shelter stay dates. The HMIS offers calculations for discrete stays as well as the total stays across multiple sheltering events.

Point in Time Count	PIT	An annual count during the last ten days in January that is required for all Continuum Designated HMIS Lead Agencies. Every year, that count also includes an "unsheltered" or street count.
Housing Inventory Chart	HIC	All residential programs (both HMIS and non-participating) must specify the number of beds and units available to homeless persons. The numbers are logged into related Provider Pages where the corresponding person data is recorded (for participating programs).
SOAR	SOAR	Using the national "best practice" curriculum, SOAR, reduces the barriers and supports the application for Social Security Benefits for disabled homeless persons.
Homeless Definition		See Homeless Definition. Hearth defines 4 categories of homelessness. Not all programs can serve all categories and some may utilize a different definition when delivering services. PromisSE has adopted the HUD definition for counting the homeless. ● Category 1: Literally Homeless ● Category 2: Imminent Risk of Homelessness ● Category 3: Homeless under other Federal Statute ● Category 4: Fleeing/Attempting to Flee DV
Projects for Assistance in Transition from Homelessness	PATH	PATH is funded by the Substance Abuse and Mental Health Services Administration (SAMHSA) administered by the Bridgeway Center Inc. It provides services to mentally ill homeless people, primarily through street outreach, to link them to permanent community housing. This program has different reporting requirements than HUD funded programs and uses HMIS to collect this information.

Permanent Supportive Housing	PSH	System that provides Permanent Supportive Housing to disabled persons throughout the catchment area and reports to the HMIS.
Okaloosa AIDS Support & Informational Services	OASIS	OASIS provides housing assistance and related supportive services for persons with HIV/AIDS and family members who are homeless or at risk of homelessness. This program has different program reporting requirements than other HUD funded programs in this document.

Coordinated Intake and Assessment		Coordinated Intake and Assessment program ensures that our area has a single or multiple point(s) of entry as well as a no wrong door policy for homeless persons.

Okaloosa Walton Homeless Continuum of Care Board of Directors- HMIS Steering Commitee		Governing Entity 1) The Steering Committee structure will be as follows: one voting seat will be provided to local, participating HMIS Agencies that have been actively using the system for 24 months; paid members of the CoC; and the voting seat will be held by the same registered voter and alternate voter on record in the membership registry. One voting seat will be provided by the HMIS Lead Agency. The Steering Committee can add non-voting advisory seats, as needed for additional partners and subject matter experts. 2) The Steering Committee will be responsible for the development and revision of the PromisSE Policies and Procedures and their enforcement, expansion of the implementation, determine the HMIS software for the CoC, determine the Lead HMIS Agency, and identify a HMIS Coordinator in addition to the Lead HMIS Agency to facilitate Bowman support. 3) The Steering Committee will meet at least quarterly with at least one meeting occurring in person. 4) The Steering Committee will identify three officers to serve a one year term and they will be as follows: a. The Steering Committee Chair will be responsible for calling and facilitating meetings, designating committees, and assigning committee duties. b. The Steering Committee Vice-Chair will be responsible for assuming the duty of the Chair in the case the Chair is unable to fulfill them.

		c. The Steering Committee Secretary will be responsible for maintaining minutes and documentation relating to the Steering Committee.

PromisSE HMIS Lead Agency		1) The Steering Committee will designate a PromisSE HMIS Lead Agency. 2) The PromisSE HMIS Lead Agency will be responsible for ascertaining contractual obligations are fulfilled relating to the HMIS software: a. Establishing a fee structure. b. Invoicing participating Local CoCs. c. Ordering End User licenses as requested by local HMIS Lead Agencies.

Policy Disclaimers and Updates

Operating Procedures defined in this document represent the minimum standards of participation in the HMIS System and general “best practice” operation procedures. Local Agencies, in coordination with their Continuum Designated HMIS Lead Agencies may include additional standards.

Operation Standards in this document are not intended to supersede grant specific requirements and operating procedures as required by funding entities. Path, OASIS and VA providers have operating rules specific to HHS and VA.

The HMIS Operating Policies and Procedures are updated routinely as HUD publishes additional guidance or as part of the annual review. Updates will be reviewed by PromisSE's HMIS LEAD AGENCY administration. To allow for evolution of compliance standards without re-issuing core agreements, updated policies supersede related policies in previously published Policies and Procedures or Agreements. Any changes from the previous year will be highlighted. A current copy of the Policy and Procedures may also be found on the PromisSE's HMIS Lead Agency's Site: www.owhcoc.org

Agreements, Certifications, Licenses and Disclaimers:

1) Each Continuum Designated HMIS Lead Agency signs an Agreement and Authorization that designates the use of a Statewide HMIS Vendor and identifies the PromisSE's HMIS Lead Agency as the lead Agency for administration of the regional database. Each Continuum Designated HMIS Lead Agency will also collaborate with PromisSE's HMIS Lead Agency. PromisSE's HMIS Lead Agency is responsible for specific tasks. The Agreement and Authorization supports the ability for multiple jurisdictions to participate on a single HMIS information System.

2) PromisSE's HMIS Lead Agency will keep all Continuum Designated HMIS Lead Agency Partnership

Agreements on file. Continuum Designated HMIS Lead Agencies will keep all PromisSE License Agreements and Agency Participation Agreements on file. Training Certifications are kept by the Continuum Designated HMIS Lead Agency, and partner Agencies are given a copy for reference and maintenance of their files.

3) All Continuum Designated HMIS Lead Agencies and Agencies must have fully executed, and be in compliance with, the following Agreements and Policies:
   a) Participation Agreement (See Appendix A for Agencies and Appendix L for Continuum Designated HMIS Lead Agencies) governing the basic operating principles of the System and rules of membership.
   b) A Board of Directors approved Confidentiality Policy governing the Privacy and Security standards for the Agency or Continuum Designated HMIS Lead Agency.
   c) User Agreement governing the individual's participation in the System.
   d) Agency Administrator Agreement for Agencies (See Appendix B) or System Administrator Agreement for Continuum Designated HMIS Lead Agencies (See Appendix M) governing the role and responsibility thereof.
   e) Security Officer Agreement (See Appendix C for Agencies or Appendix N for Continuum Designated HMIS Lead Agencies) governing the roles and responsibilities thereof.

4) Continuum Designated HMIS Lead Agencies must have an assigned System Administrator. The System Administrator:
   a) Has completed, at minimum, System Admin. training.
   b) Ensures that all Agency End Users have signed User Agreements documents on file.
   c) Ensures that all Agency Administrators have signed Agency Admin agreements on file.
   d) Ensures that all Security Officers have signed Security Officer agreements on file.

e) Ensures that all End Users complete an annual End User Certification Test, which includes Privacy and Security training.

f) Ensures that all End Users have completed workflow training and related updates, and have documentation of training.

g) Ensures that the Continuum Designated HMIS Lead Agency is in compliance with the Continuum Designated HMIS Lead Agency Data Security standards.

h) Ensures that the Continuum Designated HMIS Lead Agency is in compliance with the PromisSE Policies and Procedures.

i) Ensures that all End Users have submitted a criminal background check.

5) Agencies must have an assigned Agency Administrator. The Agency Administrator:

a) Has completed, at minimum, general ClientPoint training.

b) Ensures that all Agency End Users have signed User Agreements documents on file.

c) Ensures that all End Users will complete an annual End User Certification Test, which includes Privacy and Security training.

d) Ensures that all End Users have completed workflow training and related updates, and have documentation of training.

e) Ensures that the Agency is in compliance with the Continuum Designated HMIS Lead Agency Data Security standards.

f) Ensures that the Agency is in compliance with the HMIS Policies and Procedures, has completed the Compliance Checklist (see Appendix D), and is responsible for returning it to the local Lead Agency System Administrator.

Privacy and Security Plan:

All records entered into the HMIS and downloaded from the HMIS are required to be kept in a confidential and secure manner.

Oversight:

1) All Continuum Designated HMIS Lead Agencies must assign a System Security Officer. The System Security Officer:

   a) Ensures that all staff using the System complete annual privacy and security training. Training must be provided by PromisSE's HMIS Lead Agency and be based on the PromisSE Privacy and Security standards.

   b) Conducts an annual security review of the Continuum Designated HMIS Lead Agency that includes reviewing compliance with the Privacy and Security sections of this document. The Continuum Designated HMIS Lead Agency must document the findings of the review on the Privacy and Security Checklist (see Appendix E). The Agency must submit the findings to the Lead HMIS System Administrator no later than December 31st of each year.

   c) Notifies the Lead Agency System Administrator when a System Administrator leaves the organization or when revision of the user's access level is needed because of changes in job responsibilities. The notification must be made within 48 hours of the change.

   d) Reports any security or privacy incidents to the local Lead HMIS System Administrator for the Continuum Designated HMIS Lead Agency Jurisdiction. The System Administrator investigates the incident, including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the Continuum Designated HMIS Lead Agency. A Corrective Action Plan will be implemented. Components of the Plan must include, at minimum, supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

2) All Agencies must assign a Security Officer. The Security Officer:

a) Ensures that all staff using the System complete annual privacy and security training. Training must be provided by the local System Administrator or designated staff and be based on the PromisSE Privacy and Security standards.

b) Conducts an annual security review of the Agency that includes reviewing compliance with the Privacy and Security sections of this document. The Agency must document the findings of the review on the Privacy and Security Checklist (see Appendix E). The Agency must submit the findings to the local Lead HMIS System Administrator no later than December 31st of each year.

c) Notifies the local Lead Agency System Administrator when a staff person leaves the organization or when revision of the user's access level is needed because of a change in job responsibilities. The notification must be made within 48 hours of the change.

d) Reports any security or privacy incidents to the local Lead HMIS System Administrator for the Continuum Designated HMIS Lead Agency Jurisdiction. The System Administrator investigates the incident, including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the Continuum Designated HMIS Lead Agency. A Corrective Action Plan will be implemented. Components of the Plan must include, at minimum, supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

3) Criminal background checks must be completed on all End Users, and must be submitted to the local Lead Agency System Administrator prior to End Users gaining access to the System. For current End Users, the background check must be submitted on or before the date of the next End User Agreement (see Appendix F).

4) PromisSE's HMIS Lead Agency conducts routine audits to ensure compliance with the HMIS Policies and Procedures. The audit could include a mix of System and on-site reviews. PromisSE's HMIS Lead Agency will make recommendations for corrections as needed.

Privacy:

1) All Agencies and Continuum Designated HMIS Lead Agencies are required to have the HUD Public Notice (see Appendix H) posted and visible to clients where information is collected.

2) All Agencies and Continuum Designated HMIS Lead Agencies must have a Privacy Notice (see Appendix I). They may adopt the PromisSE sample notice or integrate the sample into their existing Notice. All Privacy Notices must define the uses and disclosures of data collected on HMIS including:

   a) The purpose for collection of client information.

   b) A brief description of Policies and Procedures governing privacy, including protections for vulnerable populations.

   c) Data collection, use and purpose limitations. The Uses of Data must include de-identified data.

   d) The client's right to copy/inspect/correct their record.

   e) The client complaint procedure.

   f) Notice to the consumer that the Privacy Notice may be updated over time and that the Privacy Notice applies to all client information held by the Agency or Continuum Designated HMIS Lead Agency.

3) All Notices must be posted on the Agency's or Continuum Designated HMIS Lead Agency's website.

4) All Agencies and Continuum Designated HMIS Lead Agencies are required to have a Privacy Policy (see Appendix J). Agencies and Continuum Designated HMIS Lead Agencies may elect to use the Sample Privacy Policy provided by PromisSE. All Privacy Policies must include:

a) Procedures defined in the Agency's or Continuum Designated HMIS Lead Agency's Privacy Notice

b) Protections afforded those with increased privacy risks such as protections for victims of domestic violence, dating violence, sexual assault, and stalking. At the Agency's or Continuum Designated HMIS Lead Agency's request, protection could include at minimum:

   i) Setting closed visibility so that only the serving Agency may see the record.

   ii) The right to have a record marked as inactive.

   iii) The right to remove their record from the System.

c) Security of hard copy files

d) Policy covers client data generated from the HMIS

e) Client Information Storage and Disposal

f) Remote Access and Usage

g) Use of Portable Storage (Significant Security Risk)

5) Agencies and Continuum Designated HMIS Lead Agencies must protect hard copy data that includes client identifying information from unauthorized viewing or access.

a) Client files are locked in a drawer/file cabinet.

b) Offices that contain files are locked when not occupied.

c) Files are not left visible for unauthorized individuals.

6) Agencies and Continuum Designated HMIS Lead Agencies must have appropriate Release(s) of Information.

a) The Agency or the Continuum Designated HMIS Lead Agency has adopted the PromisSE Release of Information (see Appendix G) as their Release.

b) The Agency or the Continuum Designated HMIS Lead Agency can integrate the PromisSE Release of Information into their existing Releases.

7) Agencies and Continuum Designated HMIS Lead Agencies are required to maintain a culture that supports privacy.

   a) Staff does not discuss client information in the presence of others without a need to know.

   b) Staff will eliminate unique client identifiers before releasing data to the public.

   c) The Agency configures intake workspaces that support privacy of client interaction and data entry.

   d) User accounts and passwords are not shared between End Users, or left visible for others to see.

   e) Program staff are educated to not save reports with client identifying data on portable media.

   f) Staff is trained regarding appropriate use of email communication.

8) All staff using the System must complete an annual End User Certification Test, which includes Privacy and Security training. Certificates documenting completion of training must be stored for review upon audit.

9) Victim Service Providers are precluded from entering client level data on the HMIS or providing client identified data to the HMIS

Data Security:

1) All licensed End Users of the System must be assigned Access Levels that are consistent with their job responsibilities and their business “need to know”.

2) All computers have virus protection with automatic updates.

   a) System Administrators or designated staff are responsible for monitoring all computers that connect to the HMIS to ensure:

      i) The Anti-Virus Software is using the up-to-date virus database.

ii) That updates are automatic.

iii) OS Updates are scheduled to run regularly.

3) All computers are protected by a Firewall.

a) System Administrators or designated staff are responsible for monitoring all computers that connect to the HMIS to ensure:

i) For Single Computers, the Software and Version is current.

ii) For Network Computers, the Firewall Model and Version is current.

iii) That updates are automatic.

4) Physical access to computers that connect to the HMIS is controlled.

a) All workstations are in secured locations (locked offices).

b) Workstations are logged off when not manned.

c) All workstations are password protected.

d) All HMIS End Users are proscribed from using a computer that is available to the public or from accessing the System from a public location through an internet connection that is not secured. That is, staff is not allowed to use Internet Cafes, Libraries, Airport Wi-Fi or other non-secure internet connections.

5) A plan for remote access if staff will be using the HMIS System outside of the office, such as doing entry from home. Concerns addressed in this plan should include the privacy surrounding the off-site entry.

a) The computer and environment of data entry must meet all the standards defined above.

b) Downloads from the computer may not include client identifying information.

c) System access settings should reflect the job responsibilities of the person using the System. Certain access levels do not allow for downloads.

Remember that your information security is never better than the trustworthiness of the staff you license to use the System. The data at risk is your own and that of your sharing partners. If an accidental or purposeful breach

occurs, you are required to notify the PromisSE's HMIS LEAD AGENCY immediately. A full accounting of access to the record can be completed.

Disaster Recovery Plan:

The HMIS can be a critically important tool in the response to catastrophic events. The HMIS data is housed in a secure server bank in Shreveport, LA with nightly off-site backup. This means that data is immediately available via Internet connection if the catastrophe is in the PromisSE implantation and can be restored within 4 hours if the catastrophe is in Louisiana.

1) HMIS Data System (see "Bowman Systems Securing Client Data" for a detailed description of data security and Bowman's Disaster Response Plan):
   a) PromisSE is required to maintain the highest level disaster recovery service by contracting with Bowman Systems for Disaster Recovery that includes:
      i) Off site, out-of-state, on a different Internet provider and on a separate electrical grid, backups of the application server via a secured Virtual Private Network (VPN) connection.
      ii) Near-Instantaneous backups of application site (no files older than 5 minutes)
      iii) Nightly off site replication of database in case of a primary data center failure.
      iv) Priority level response (ensures downtime will not exceed 4 hours).
2) Communication between staff of PromisSE's HMIS Lead Agency, the Continuum Designated HMIS Lead Agency, and the Agencies in the event of a disaster is a shared responsibility and will be based on location and type of disaster.

System Administration and Data Quality Plan:

1) Provider Page Set-Up:

   a) Provider Pages are appropriately named per the FL-505 (CoC #) naming standards <CoC Name> - <Program Type><Agency name> - <Program Name>.

   Example: "501AL-(TH)Housing First - Victory".

   b) Inactive Provider Pages are properly identified with "ZZZ"><Provider Page Name.

   c) Provider Pages maintained from CommunityPoint, but not used by the local Lead HMIS Agency, are properly identified with "Database Only" >Provider Page Name.

   d) HUD Data Standards are fully completed on all Provider Pages:

      i) CoC code is set correctly.

      ii) Program type codes are set correctly.

      iii) Geocodes are set correctly.

      iv) Bed and Unit Inventories are set for applicable residential programs.

   e) The local Lead Agency System Administrator is responsible for setting up and maintaining Provider pages.

2) Data Quality Plan:

   a) Continuum Designated HMIS Lead Agencies must require documentation at intake of the homeless status of clients according to the reporting and eligibility guidelines issued by HUD. The "order of priority" for obtaining evidence of homeless status is (1) third party documentation, (2) worker observations, and (3) certification from the person. Lack of third party documentation may not be used to refuse emergency shelter, outreach or domestic violence services. 100% of the clients must be entered into the System within 48 hours of Intake.

b) All staff are required to be trained on the definition of Homelessness.

   i) There is congruity between the following HMIS case record responses, based on the applicable homeless definition: (Is Client Homeless, Housing Status and Prior Living Situation are being properly completed).

c) Continuum Designated HMIS Lead Agency has a process to ensure the First and Last Names are spelled properly and the DOB is accurate.

   i) An ID is requested at intake to support proper spelling of the client's name and accurate recording of the DOB.

   ii) If no ID is available, staff will request the legal spelling of the client's name.

   iii) Programs that serve the chronic and higher risk populations are encouraged to use the Scan Card process within ServicePoint to improve un-duplication and to improve the efficiency of recording services.

d) Income and non-cash benefits are being updated at least annually and at exit for Emergency Shelters, and at least quarterly through Interim Reviews and Follow Up Reviews for all other program types.

e) Continuum Designated HMIS Lead Agencies have an organized exit process that includes:

   i) Clients and staff are educated on the importance of planning and communicating regarding discharge.

   ii) Discharge Destinations are properly mapped to the HUD Destination Categories.

   iii) There is congruity between discharge destination and Housing Status at exit.

   iv) There is a procedure for communicating exit information to the person responsible for data entry.

f) System Administrators will run data quality reports on a monthly basis, unless mandated at a higher rate by individual grant requirements.

i) Report frequency for funded programs will be governed by Grant Agreements, HUD reporting cycles, and local Continuum Designated HMIS Lead Agency Standards. However, all programs will be reviewed and asked to make corrections at least monthly.

ii) Data quality screening and correction activities must include the following:

(1) Missing or inaccurate information in (red) Universal Data Element Fields.

(2) Un-exited clients using the Length of Stay and Un-exited Client Data Quality Reports.

3) Workflow Requirements:

a) Assessments set in the Provider Page Configuration are appropriate for the funding stream.

b) End Users performing data entry have latest copies of the workflow guidance documents.

c) If using paper, the intake data collection forms correctly align with the workflow.

d) 100% of clients are entered into the System within 48 hours of intake.

e) Continuum Designated HMIS Lead Agencies are actively monitoring program participation and existing clients. Clients are exited within 30 days of last contact unless program guidelines specify otherwise.

f) All required program information is being collected.

i) All HMIS participants are required to enter at minimum the Universal Data Elements as well as the program specific entry/exit form.

ii) Programs that serve over time are required to complete additional program elements as defined by the funding stream.

g) Data sharing is properly configured for sharing information internally between programs, including use of visibility groups.

h) External data sharing aligns with any local, state or Federal laws; including use of visibility groups.

4) Electronic Data Exchanges:

a) Agencies requesting the ability to import or export data from the HMIS must receive permission from the local Lead Agency before doing so.

b) Continuum Designated HMIS Lead Agencies may elect to participate in de-identified research data sets to support research and planning.

   i) De-identification will involve the masking or removal of all identifying or potential identifying information such as the name, Unique Client ID, SS#, DOB, address, Agency name, and Agency location.

   ii) Geographic analysis will be restricted to prevent any data pools that are small enough to inadvertently identify a client by other characteristics or combination of characteristics.

   iii) Programs used to match and/or remove identifying information will not allow a re-identification process to occur. If retention of identifying information is maintained by a "trusted party" to allow for updates of an otherwise de-identified data set, the organization/person charged with retaining that data set will certify that they meet medical/behavioral health security standards and that all identifiers are kept strictly confidential and separate from the de-identified data set.

   iv) Continuum Designated HMIS Lead Agencies will be provided a description of each Study being implemented when including data from that Continuum Designated HMIS Lead Agency. Continuum Designated HMIS Lead Agencies may opt out of the Study through a written notice to the requesting Continuum Designated HMIS Lead Agency.

5) Staff Training and Required Meetings:

   a) All End Users are recertified through the End User Certification Test annually.

   b) All End Users participate in Workflow Training and Training Updates for their assigned Workflows.

   c) All End Users will receive the list of HUD Data Standards Universal Data Elements (see Appendix K).

Appendix A

Agency Participation Agreement

Okaloosa Walton Homeless Continuum of Care Program Management Information System Participation Agreement Between the CoC and

_____

(Name of Agency)

This agreement is entered into on _____ (dd/mm/yy) between the CoC, hereafter known as the CoC, and _____

(Agency name), hereafter known as "Agency," regarding access and use of the CoC Program Management Information System South East, hereafter known as "***PromisSE***."

I. Introduction

The ***PromisSE***, a shared human services database, allows authorized personnel at homeless and human service provider agencies throughout the participating regions of the Southeast enter, track, and report on information concerning their own clients and to share information, subject to appropriate inter-Agency agreements, on common clients.

***PromisSE*'s** goals are to:

- Improve coordinated care for and services to homeless persons in the states of Alabama and Florida.
- Provide a user-friendly and high quality automated records System that expedites client intake procedures, improves referral accuracy, increases case management and administrative tools, creates a tool to follow demographic trends and service utilization patterns of families and individuals either currently experiencing or about to experience homelessness, and supports the collection of quality information that can be used for program improvement and service-planning.
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD) and other funders as needed.

In compliance with all State and Federal requirements regarding client confidentiality and data security, the ***PromisSE*** is designed to collect and deliver timely, credible, quality data about services and homeless persons or persons at risk for being homeless. the CoC administers the ***PromisSE*** through a contract with HUD.

II. CoC Responsibilities

1. The CoC will provide the Agency 24-hour access to the ***PromisSE*** data-gathering System via internet connection, with which the Agency is responsible for maintaining connectivity.
2. The CoC will provide model Privacy Notices, Client Release forms and other templates for agreements that may be adopted or adapted at the participating Agency.
3. The CoC will provide both initial training and periodic updates to that training for core Agency staff regarding the use of the ***PromisSE***, with the expectation that the Agency will take responsibility for conveying this information to all Agency staff using the System.
4. The CoC will provide basic user support and technical assistance (i.e., general trouble-shooting and assistance with standard report generation). Access to this basic technical assistance will normally be available from 8:30 AM. to 4:30 PM. on Monday through Friday (with the exclusion of holidays) and limited availability after regular hours.

5. The CoC will not publish reports on client data that identify specific agencies or persons, without prior Agency (and where necessary, client) permission. Public reports otherwise published will be limited to presentation of aggregated data within the ***PromisSE*** database.

III. AGENCY Responsibilities

1. The Agency will comply with the CoC Homeless Management Information System (HMIS) Operating Policy and Procedure.
2. The Agency will designate and staff one HMIS Agency Administrator who shall abide by the policies and procedures set out in the CoC Homeless Management Information System (HMIS) Operating Policy and Procedure.
3. The Agency will designate and staff one HMIS Security Officer who shall abide by the policies and procedures set out in the CoC Homeless Management Information System (HMIS) Operating Policy and Procedure.
4. The Agency will ensure that both initial training and periodic updates to that training for core Agency staff regarding the use of the ***PromisSE*** is completed in accordance with the requirements set out in the CoC Homeless Management Information System (HMIS) Operating Policy and Procedure.

IV. Privacy and Confidentiality

A. Protection of Client Privacy

1. The Agency will comply with all applicable Federal and State laws regarding protection of client privacy.
2. The Agency will comply specifically with Federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records. A general authorization for the release of medical or other information is NOT sufficient for this purpose. Member Agencies shall recognize that Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
3. The Agency will comply specifically with the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human Services.
4. The Agency will comply with all policies and procedures established by the CoC pertaining to protection of client privacy.
5. Each Member Agency will abide specifically by Alabama and Florida State Laws, which in general terms, require an individual to be informed that any and all medical records she/he authorizes to be released, whether related to physical or mental health, may include information indicating the presence of a communicable or venereal disease. The Agency is required to inform the individual that these records may include, but are not limited to, the inclusion of information on diseases such as hepatitis, syphilis, gonorrhea, tuberculosis, and HIV/AIDS.
6. Each Member Agency will abide specifically by local Mental Health Law. In general terms, this law prohibits agencies from releasing any information that would identify a person as a client of a mental health facility, unless client consent is granted.

B. Client Confidentiality

1. The Agency agrees to provide a copy of the CoC Privacy Notice (or an acceptable Agency specific alternative) to each client. The Agency will provide a verbal explanation of the ***PromisSE*** and arrange for a qualified interpreter/translator in the event that an individual is not literate in English or has difficulty understanding the Privacy Notice or associated Consent Form(s).

2. The Agency will not solicit or enter information from clients into the ***PromisSE*** database unless it is essential to provide services or conduct evaluation or research.
3. The Agency will not divulge any confidential information received from the ***PromisSE*** to any organization or individual without proper written consent by the client, unless otherwise permitted by applicable regulations or laws.
4. The Agency will ensure that all persons who are issued an End User Identification and Password to the ***PromisSE*** abide by this Participation Agreement, including all associated confidentiality provisions. The Agency will be responsible for oversight of its own related confidentiality requirements.
5. The Agency agrees that it will ensure that all persons issued an End User ID and Password complete a formal training on privacy and confidentiality, demonstrate mastery of that information, and sign a ***PromisSE*** End User Agreement prior to activation of the End User License.
6. The Agency acknowledges that ensuring the confidentiality, security and privacy of any information downloaded from the System by the Agency is strictly the responsibility of the Agency.

C. Inter-Agency Sharing of Information

1. The Agency acknowledges that all forms provided by ***PromisSE*** regarding client privacy and confidentiality are shared with the Agency as generally applicable models that may require specific modification in accord with Agency-specific rules. The Agency will review and revise (as necessary) all forms provided by ***PromisSE*** to assure that they are in compliance with the laws, rules and regulations that govern its organization.
2. The Agency acknowledges that informed client consent is required before any basic identifying client information is shared with other Agencies in the System. The Agency will document client consent on the ***PromisSE*** Client Release of Information Form.
3. If the client has given approval through a completed ***PromisSE*** Client Release of Information Form, the Agency may elect to share information with other partnering agencies in ***PromisSE***.
4. The Agency will incorporate a ***PromisSE*** release clause into its existing Agency Authorization for Release of Information Form(s) if the Agency intends to share restricted client data within the ***PromisSE***. Restricted information, including progress notes and psychotherapy notes about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall <u>not</u> be shared with other participating Agencies without the client's written, informed consent. Agencies with visibility set to "closed" may not share "closed" client information without the client's written, informed consent, as well as a fully executed inter-Agency "closed" data sharing agreement.
5. Agencies with which information is shared are each responsible for obtaining appropriate consent(s) before allowing further sharing of client records. Any sharing of "closed" data will be facilitated in the ***PromisSE*** by the local System Administrator, and will be initiated after the
   System Administrator's receipt of the fully executed inter-Agency "closed" data sharing agreement.
6. The Agency acknowledges that the Agency itself bears primary responsibility for oversight of the sharing of all data it has collected via the ***PromisSE***.
7. The Agency agrees to place all Client Authorization for Release of Information forms related to the ***PromisSE*** in a file to be located at the Agency's business address and that such forms will be made available to the CoC for periodic audits. The Agency will retain these ***PromisSE***-related Authorizations for Release of Information forms <u>for a period of 7 years</u>, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.

8. The Agency acknowledges that clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.

D. Custody of Data

1. The Agency and the CoC understand that the Agency and the CoC as administrator are custodians – NOT owners - of the data.
2. In the event that the ***PromisSE*** Project ceases to exist, Member Agencies will be notified and provided reasonable time to access and save client data on those served by the Agency, as well as statistical and frequency data from the entire System. Thereafter, the information collected on the centralized server will be purged or appropriately stored.
3. In the event that the CoC ceases to exist, the custodianship of the data within ***PromisSE*** will be transferred to another authorized organization for continuing administration, and all ***PromisSE*** Member Agencies will be informed in a timely manner.

V. Data Entry and Regular Use of *PromisSE*

1. The Agency will not permit End User IDs and Passwords to be shared among End Users.
2. If a client has previously given the Agency permission to share information with multiple agencies (beyond basic identifying information and non-restricted service transactions), and then chooses to revoke that permission with regard to one or more of these agencies, the Agency will contact its partner Agency/agencies and explain that, at the client's request, portions of that client record will no longer be shared. The Agency will then "lock" those portions of the record impacted by the revocation to the other Agency or agencies.
3. If the Agency receives information that necessitates a client's information be entirely removed from the ***PromisSE***, the Agency will work with the client to complete a brief Delete Request Form, which will be sent to the CoC for de-activation of the client record.
4. The Agency will enter all minimum required data elements as defined for all persons who are participating in services funded by the U.S. Department of Housing and Urban Development (HUD) Supportive Housing Program, Shelter + Care Program, or HUD Emergency Shelter Grant Program.
5. The Agency will enter data in a consistent manner and will strive for real-time, or close to real-time, data entry.
6. The Agency will routinely review records it has entered in the ***PromisSE*** for completeness and data accuracy. The review and data correction process will be made according to ***PromisSE*** published Data Quality Policies and Procedures.
7. The Agency will not knowingly enter inaccurate information into ***PromisSE***, with the exception of DV providers where Agency is permitted to input coded data into the System.
8. The Agency acknowledges that with a current standard ***PromisSE*** Client Release of Information form on file, it can update, edit, and print out a client's information. Once the ***PromisSE*** Client Release of Information expires, the Agency can no longer edit or print the record.
9. The Agency acknowledges that once that Client Release of Information expires, any new information entered into the database will be closed to sharing until a new Client Release of Information is signed. Information entered before the date of the expired release will continue to be available to the sharing partners.

10. The Agency acknowledges that a modified Agency Authorization to Release Information form, with a ***PromisSE*** clause, permits it to share restricted client information with select agencies in compliance with the Agency's approved Confidentiality Policies and Procedures.
11. The Agency will prohibit anyone with an Agency-assigned End User ID and Password from entering offensive language, profanity, or discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation.
12. The Agency will utilize the ***PromisSE*** for business purposes only.
13. The Agency will keep updated virus protection software on Agency computers that access the ***PromisSE***.
14. Transmission of material in violation of any United States Federal or State regulations is prohibited.
15. The Agency will not use the ***PromisSE*** with intent to defraud the Federal, State, or local government, or an individual entity, or to conduct any illegal activity.
16. The Agency agrees that the ***PromisSE*** or the local Continuum of Care ***PromisSE*** Planning Committee may convene local or regional End User Meetings to discuss procedures, updates, policy and practice guidelines, data analysis, and software/ hardware upgrades. The Agency will designate at least one specific Staff member to regularly attend End User Meetings.

19. Notwithstanding any other provision of this Participation Agreement, the Agency agrees to abide by all policies and procedures relevant to the use of ***PromisSE*** that the CoC publishes from time to time.

VI. Publication of Reports

1. The Agency agrees that it may release only aggregated information generated by the ***PromisSE*** that is specific to its own services.

VII. Database Integrity

1. The Agency will not share assigned End User IDs and Passwords to access the ***PromisSE*** with any other organization, governmental entity, business, or individual.

2. The Agency will not intentionally cause corruption of the ***PromisSE*** in any manner. Any unauthorized access or unauthorized modification to computer System information or interference with normal System operations will result in immediate suspension of services, and, where appropriate, legal action against the offending entities.

VIII. HMIS Fee Schedule

1. The CoC has adopted the CoC HMIS fee schedule for all participating Agencies.
2. The CoC, as the lead Agency, will provide the specified amount of End User licensing, training, technical assistance, and other services or activities relevant to the participation in ***PromisSE*** as listed in the CoC HMIS fee schedule.
3. The Agency will remunerate the CoC per End User for missed training and per End User for reactivation of an inactive license as set out in the CoC HMIS fee schedule.

VIIII. Hold Harmless

1. The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws,

statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the Agency's or other member Agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

2. It is the responsibility of each Agency to maintain a current insurance policy that is sufficient to cover theft of or damage to ALL ***PromisSE*** -related hardware and software.

X. Terms and Conditions

1. The parties hereto agree that this agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.
2. The Agency shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of the CoC.
3. This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term occurs if allegations or actual incidences arise regarding possible or actual breeches of this agreement. Should such situations arise, the ***PromisSE*** System Administrator may immediately suspend access to ***PromisSE*** until the allegations are resolved in order to protect the integrity of the System.
4. This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.
5. The parties agree that the CoC, Inc. is a third-party beneficiary of this contract and may enforce the terms and provisions of this contract as applicable.

IN WITNESS WHEREOF, the parties have entered into this Agreement:

Okaloosa Walton Homeless Continuum of Care
207 Hospital Drive NE, Suite B.
Fort Walton Beach, FL 32548

_____	_____
OWHCoC Telephone Number	HMIS Lead Agency Telephone Number
_____	_____
OWHCoC Representative Printed Name	HMIS Lead Agency Representative Printed Name
_____	_____
OWHCoC Representative Title	HMIS Lead Agency Representative Title
_____	_____
OWHCoC Representative Signature	HMIS Lead Agency Representative Signature
_____/_____/_____	_____/_____/_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix A

Agency Participation Agreement

APPENDIX A

Assurance

Okaloosa Walton Homeless Continuum of Care Program Management Information System
ASSURANCE

_____ (Name of Agency) assures that the following fully executed documents will be on file and available for review.

- ✓ The Agency's official Privacy Notice for ***PromisSE*** clients.
- ✓ Executed ***PromisSE*** Client Release of Information forms.
- ✓ Executed Agency Authorizations for Release of Information as needed.
- ✓ Certificates of Completion for required training for all ***PromisSE*** System End Users.
- ✓ A fully executed End User Agreement for all ***PromisSE*** System End Users.
- ✓ A current Agency-Specific ***PromisSE*** Policy and Procedure Manual.

By: _____

Title: _____

Signature: _____

Date: _____

APPENDIX B

Agency Administrator Agreement

CoC Agency Administrator Agreement

Name:_____
Agency Name:_____

All HMIS participating agencies must designate and staff one HMIS Agency Administrator. Agency Administrator requirements and responsibilities include, but are not limited to, the following:

- Has completed, at minimum, general ClientPoint training.
- Ensure that all Agency users have signed End User Agreement documents on file.
- Ensure that all Users complete an annual End User Certification Test, which includes Privacy and Security training.
- Ensure that all Users have completed workflow training and related updates, and have documentation of training.
- Ensure that the Agency is in compliance with the CoC Data Security standards.
- Ensure that the Agency is in compliance with the HMIS Policies and Procedures, has completed the Compliance Checklist, and is responsible for returning it to the local Lead Agency System Administrator.
- Ensure that all Users have submitted a criminal background check to the local Lead Agency System Administrator.

The original Agency Administrator Agreement shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after date of signing. Agency Administrators are required to complete HMIS End User Certification testing and to document compliance monitoring annually, at which time a new agreement will be provided. Failure to participate in annual Certification and/or maintain a current agreement may result in immediate termination or suspension of the user's ServicePoint license and access to ServicePoint. Failure to comply with the provisions of this Agency Administrator Agreement is grounds for immediate termination. Your signature below indicates your agreement to comply with this Agency Administrator Agreement.

_____	_____
Employee Printed Name	Agency Official Printed Name
_____	_____
Employee Signature	Agency Official Signature
_____	_____
Date (mm/dd/yy)	Date (mm/dd/yy)

APPENDIX C

CoC Security Officer Agreement

Name:_____

Agency Name:_____

All HMIS participating agencies must designate and staff one HMIS Security Officer. Security Officer requirements and responsibilities include, but are not limited to, the following:

- Ensures that all staff using the system complete annual privacy and security training. Training must be provided by the CoC designated trainers and be based on the CoC Privacy and Security standards.
- Conducts an annual security review of the agency that includes reviewing compliance with the Privacy and Security sections of the CoC Homeless Management Information System (HMIS) Operating Policy and Procedure. The Agency must document the findings of the review on the Privacy and Security Checklist and submit the findings to the HMIS System Administrator no later than December 31 of each year.
- Notifies the local Lead Agency System Administrator when a staff person leaves the organization or when revision of the user's access level is needed because of a change in job responsibilities. The notification must be made within 48 hours of the change.
- Reports any security or privacy incidents to the local Lead HMIS System Administrator for the CoC Jurisdiction. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the CoC. A Corrective Action Plan will be implemented. Components of the Plan must include, at minimum, supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

The original Security Officer Agreement shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after date of signing. Security Officers are required to complete HMIS End User Certification testing and documented Privacy & Security compliance monitoring annually, at which time a new agreement will be provided. Failure to participate in annual Certification, Privacy & Security monitoring, and/or maintain a current agreement may result in immediate termination or suspension of the user's ServicePoint license and access to ServicePoint. Failure to comply with the provisions of this Security Officer Agreement is grounds for immediate termination. Your signature below indicates your agreement to comply with this Security Officer Agreement.

_____	_____
Agency Official Printed Name	Employee Printed Name
_____	_____
Agency Official Signature	Employee Signature
_____/_____/_____	_____/_____/_____
Date (mm/dd/yy)	Date (mm/dd/yy)

APPENDIX D

Compliance Checklist

Continuum of Care

Policies and Procedures Compliance Checklist

Agency Name:_____

_____ (Int.) Agency has received a copy of the CoC Operating Policies and Procedures
_____ (Int.) Agency has a fully executed Agency Participation Agreement
_____ (Int.) Agency has a Board approved Confidentiality Policy governing HMIS Privacy and Security Standards
_____ (Int.) Agency has assigned an HMIS Agency Administrator with executed agreement
_____ (Int.) Agency has assigned an HMIS Security Officer with executed agreement
_____ (Int.) Agency has submitted all End User criminal background checks
_____ (Int.) Agency has provided End Users with the HUD Data Elements
_____ (Int.) Agency has provided End User with training on the HUD definition of homelessness and the priority of homelessness documentation
_____ (Int.) Agency and End Users understand and will comply with the CoC Data Quality Plan

_____	_____
Agency Official Printed Name	CoC Official Printed Name
_____	_____
Agency Official Signature	CoC Official Signature
_____	_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Continuum of Care
Privacy and Security Checklist

Agency Name:_____

Security Officer Name: _____

_____ (Int.) **Agency has the HUD Public Notice posted in an area visible to clients.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **Agency has an HMIS Privacy Notice that complies with the requirements set forth by the CoC HMIS Operating Policies and Procedures, and is available to all clients.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

APPENDIX E

Privacy and Security Checklist

_____ (Int.) **Agency has a copy of the HUD Public Notice and the Privacy Notice on its website.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **Client files with hard copy data that includes client identifying information is protected behind one lock, at minimum, from unauthorized access.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **Offices that contain client files are locked when not occupied.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

APPENDIX E

Privacy and Security Checklist

_____ (Int.) **Client files are not left visible for unauthorized individuals.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **Agency has adopted the PromisSE Release of Information and requests this from every client.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **HMIS workspaces are configured to support privacy of client interaction and privacy of data entry.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

APPENDIX E

Privacy and Security Checklist

_____ (Int.) **User accounts and passwords are not shared between End Users, or left visible for others to see.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **End Users do not save HMIS reports with identifying client information on portable media.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **All HMIS workstations, including laptops and remote workstations, have virus protection and automatic updates.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

APPENDIX E

Privacy and Security Checklist

Deadline for Completion: _____

_____ (Int.) **All HMIS workstations, including laptops and remote workstations, are protected by a Firewall.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **End Users are not accessing the HMIS on a public computer, or from an internet connection that is not secured.**

Finding(s): _____

_____

_____

Corrective Action(s): _____

_____

_____

Deadline for Completion: _____

_____ (Int.) **Agency has a documented plan for remote access if End Users are accessing the HMIS outside of the office setting.**

Finding(s): _____

_____

_____

Corrective Action(s)_____

APPENDIX E

Privacy and Security Checklist

_____

_____

Deadline for Completion: _____

_____	_____
Security Officer Printed Name	Agency Official Printed Name
_____	_____
Security Officer Signature	Agency Official Signature
_____	_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix F

License Agreement

PromisSE License Agreement & Statement of Confidentiality

Name:_____

Employees, volunteers, staff and any persons with access to the **Program Management Information System South East *(PromisSE)*** are subject to certain guidelines regarding its use. *PromisSE* contains a wide range of personal and private information on individuals and ALL such information must be treated carefully, confidentially, and professionally by those who access it. Guidelines for use of *PromisSE* include, but are not limited to, the following:

- User IDs and passwords must be kept secure and confidential and shall not be shared.
- Current client or Legal Guardian consent, as documented by a Release of Information (ROI), is required before entering, updating, editing, printing, or disclosing basic identifying and non-confidential service transactions/information with other Member Agencies and/or their employees, volunteers and/or staff. Otherwise, limited visibility must be coordinated with the CoC.
- Only general, non-confidential information is to be entered in the "other notes/comments" section of the Client Profile in *PromisSE.* Confidential information, including TB diagnosis, domestic violence and mental/physical health information shall not be entered in this section.
- Confidential information obtained via *PromisSE* is to remain confidential, even if the end user's relationship with the Agency changes or concludes for any reason.
- Information beyond basic identifying data, which includes all assessment screens (all screens beyond profile, agency, and community fields), is not to be edited. If an update or correction is needed, a new assessment must be created.
- The agency/organization end user is allowed to enter or modify data ONLY for clients being served by that agency / organization.
- Misrepresentation of the client through the deliberate entry of inaccurate information is prohibited.
- Client records shall NOT be deleted from *PromisSE.* If a client or legal guardian of a client chooses to rescind *PromisSE* Release of Information, the appropriate record shall immediately become "inactive".
- Discriminatory comments based on race, color, religion, creed, national origin, ancestry, handicap, socioeconomic status, marital status, age, gender, and/or sexual orientation are NOT permitted in *PromisSE.* Profanity and offensive language are NOT permitted in *PromisSE.* Violators shall have their system privileges revoked and they will NOT be allowed further access to HMIS.
- *PromisSE* is to be used for business purposes only. Transmission of material in violation of any United States Federal or State of Alabama regulation/laws is prohibited, including material that is copyrighted, legally judged to be threatening or obscene, and/or considered protected by trade secret. *PromisSE* shall NOT be used to defraud the Federal, State, Local or City government nor any individual entity nor to conduct any illegal activity.
- Users must log off of ServicePoint before leaving their computer / workstation unattended; Failure to log off ServicePoint appropriately may result in a breach in client confidentiality and system security.
- Hard copies of ServicePoint information must be kept in a secure file.
- When hard copies of ServicePoint information are no longer needed, they must be properly destroyed to maintain confidentiality.
- Any unauthorized access or unauthorized modification to computer system information/*PromisSE* database or interference with normal system operations will result in immediate suspension of your access to the *PromisSE* and may jeopardize your employment status with the Agency.

I agree to maintain a subscription to the PromisSE email list and discussion group to receive official communications regarding PromisSE.

The original PromisSE License Agreement & Statement of Confidentiality shall be kept on file at the Agency. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

The CoC makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold the CoC harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the

Agency or another party arising from participation in the ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold the CoC harmless for loss

or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The CoC shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of the CoC. The CoC agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the CoC.

This agreement is in effect for a period of one (1) year after date of signing. End users are required to complete HMIS End User Certification testing annually, at which time a new agreement will be provided. Failure to participate in annual Certification and/or maintain a current agreement may result in immediate termination or suspension of the user's ServicePoint license and access to ServicePoint. Failure to comply with the provisions of this Statement of Confidentiality is grounds for immediate termination. Your signature below indicates your agreement to comply with this Statement of Confidentiality.

_____	_____
Employee Printed Name	Agency Official Printed Name
_____	_____
Employee Signature	Agency Official Signature
_____	_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix G

Release of Information

Continuum of Care (CoC)
Program Management Information System of the Southeast (PromisSE)

Client's Last Name: _____ First Name: _____ MI:___

Date of Birth: _____ Social Security Number: _____

*** The Federal Privacy Act of 1974 requires that you be notified that disclosure of your Social Security number is voluntary under this record-keeping system. This system was authorized pursuant to directives from Congress and the Department of Housing and Urban Development (HUD). The Social Security number is used to verify identity, assure timely delivery of services, prevent duplication of services, and generate accurate required reports to HUD.**

The PromisSE is a shared, computerized record keeping system that captures information about people experiencing homelessness or near homelessness, including their service needs. Our Agency, _____, is participating in PromisSE that collects information on clients served by its member agencies and the services they provide.

I understand that all information gathered about me is personal and private and that I do not have to share information collected in PromisSE. It has been explained to me that all information collected will serve for reporting purposes and as a precaution to prevent duplication of services to ineligible individuals and families. I have had an opportunity to ask questions about PromisSE and to review the identifying information, which is authorized by this release for the PromisSE Member Agencies to share. I also understand that information about non-confidential services provided to me by human service agencies in the CoC may be shared with other participating in PromisSE agencies. This Release of Information will remain in effect for 5 (five) years and will expire on _____ unless I make a formal request to this Agency that I no longer wish to participate in PromisSE.

- □ I authorize to share my data
- □ I do not authorize to share my data

The CoC, as PromisSE Member Agency, to share my information between all participating PromisSE agencies. I authorize the use of a copy of this original to serve as an original for the purposes stated above.

_____
Client's (Head of Household) Printed

Date (mm/dd/yy)

_____
Other Adult in HH Printed Name

_____
Client's (Head of Household) Signature

_____
Other Adult in HH Signature

_____

_____

Date (mm/dd/yy)

Appendix G

Release of Information

Page Two

Based on the above information,

- □ I authorize to share my dependents' data
- □ I do not authorize to share my dependents' data

The CoC, as PromisSE Member Agency, to share my information between all participating PromisSE agencies. I authorize the use of a copy of this original to serve as an original for the purposes stated above.

Dependent Name First, Middle Initial, Last	**Date of Birth**

_____ _____

Legal Guardian Printed Name Agency Representative Printed Name

_____ _____

Legal Guardian Authorized Signature Agency Representative Signature

_____/_____/_____ _____/_____/_____

Date (mm/dd/yy) Date (mm/dd/yy)

Appendix H

Public Notice

Public Notice

Continuum of Care

Program Management Information System of the Southeast (PromisSE)

aka: Homeless Management Information System (HMIS)

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless and at-risk persons, and to better understand the needs of homeless and at-risk persons. We only collect information that we consider to be appropriate.

The collection and use of all personal information is guided by strict standards of confidentiality. A copy of our Privacy Notice describing our privacy practice is available to all clients upon request.

Sample Privacy Notice to Clients

CoC Homeless Management Information System

Privacy Notice

The Homeless Management Information System (HMIS) was developed to meet a data collection requirement made by the United States Congress to the Department of Housing and Urban Development (HUD). Congress passed this requirement in order to get a more accurate count of individuals who are homeless and to identify the need for and use of different services by those individuals and families. Several CoCs in the Southeast share a single HMIS implementation. The CoC Lead Entity designates the HMIS Lead Agency for that CoC. Many Agencies in this area use the HMIS to keep computerized case records. With client permission as indicated by a signed Release of Information, client information can be shared with other HMIS participating Agencies throughout the Implementation. The information entered by participating providers and shared with client consent includes: basic identifying demographic data (e.g., name, birth date, and gender), the nature of the client's situation, and the services and referrals received from the participating Agency.

Participating Agencies collect personal information directly from you for reasons that are discussed in their privacy notice. They may be required to collect some personal information by law or by the organizations that give money to operate their program. Other personal information that is collected is important to operate programs, to improve services, and to better understand client needs. They only collect information that they consider to be appropriate and accurate. The collection and use of all personal information is guided by strict standards of confidentiality.

Appendix I

Sample Privacy Notice

Maintaining the privacy and safety of those clients whose records reside in HMIS and the agencies that use the HMIS is very important to us. Information gathered about each client and each Agency is personal and private. We collect information only when appropriate to provide services, manage our organization and the Database, or as required by law. The ownership of all records contained within the HMIS is retained by the organization/Agency that collected and entered or updated the client's information.

CONFIDENTIALITY RIGHTS

Each participating Agency is required to have a confidentiality policy that has been approved by its Board of Directors. _____(HMIS Lead Entity) must also have a Board Approved confidentiality policy. _____(HMIS Lead Entity) operates the HMIS in accordance with HUD and HIPAA confidentiality regulations, including those covering programs that receive HUD funding for homeless services (Federal Register/Vol. 69, No. 146), and those covered under the HIPAA privacy and security rules which govern confidential health information such as the diagnosis, treatment, of a mental health disorder, a drug or alcohol disorder, and AIDS/HIV condition or a domestic violence situation. Other rules that may also apply include 42 CFR Part 2 governing drug and alcohol records.

_____(CoC #) is restricted to using or disclosing personal information from the HMIS to the following circumstances:

- For functions related to payment or reimbursement for services.
- For functions related to helping Agencies operate the System.
- For functions related to the development of reports to better plan services.
- To carry out administrative functions including but not limited to: legal, audit, personnel, planning, oversight and management functions;
- To develop databases used for research, where all identifying information has been removed.

- To support contractual research where privacy conditions are met with an approved Institutional Review Board (IRB), and only if the shared information includes no identifying information about the client.
- Where a disclosure is required by law and disclosure complies with, and is limited to, the requirements of the law. Instances where this might occur are during a medical emergency, to report a crime against staff of the Agency, or to avert a serious threat to health or safety.

YOUR INFORMATION RIGHTS

All requests for client personal information located within the HMIS will be routed to the Agency/organization that collected and entered or updated the information.

_____(CoC #) may not disclose your personal protected information located within the HMIS except as required by law or to help the participating Agency/organization that collected/entered/updated the information operate the System.

_____(CoC #) may not publish reports on client data that identifies specific Agencies or persons. Public reports otherwise published will be limited to the presentation of aggregated data that does not disclose personal identifying information.

Please contact the Agency to which you gave your personal information in order to:

- Access or see your record.
- Correct your record
- Request that your record by shared with another person or organization.
- Terminate or withdraw consent to release information.
- File a grievance if you feel that your rights have been violated.

Please note that you have the right to refuse consent to share your information between participating Agencies. You cannot be denied services that you would otherwise qualify for if you refuse to share information. Please note that if you refuse this permission, information will

still be entered into the System for statistical purposes, but your information will be closed so that only that Agency you gave the information to and System Administrators operating the Database may see your information.

Please feel free to contact us if you feel that your information rights have been violated. Please address your written communication to the CoC (Enter Contact Information). Please include your contact information. We will respond in writing within 7 working days of the receipt of your letter.

HOW YOUR INFORMATION WILL BE KEPT SECURE

Protecting the safety and privacy of individuals receiving services and the confidentiality of their records is of paramount importance to us. Through training, policies and procedures, and software we have done several things to make sure your information is kept safe and secure:

- The computer program we use has the highest degree of security protection available.
- Only trained and authorized individuals will enter or view your personal information.
- Your name and other identifying information will not be contained in HMIS reports that are issued to local, state, or national Agencies.
- Employees receive training in privacy protection and agree to follow strict confidentiality standards before using the system.
- The server/database/software only allows authorized individuals access to the information. Only those who should see certain information will be allowed to see that information.
- The server/database will communicate using 128-bit encryption – an Internet technology intended to keep information private while it is transported back and forth across the Internet. Furthermore, identifying data stored on the server is also encrypted or coded so that it cannot be recognized.
- The server/database exists behind a firewall –a device meant to keep hackers/crackers/viruses/etc. away from the server.
- The main database will be kept physically secure, meaning only authorized personnel will have access to the server/database.

- System Administrators employed by _____ (HMIS Lead Agency) support the daily operation of the database. Administration of the database is governed by agreements that limit the use of personal information to providing administrative support and generating reports using aggregated information. These agreements further ensure the confidentiality of your personal information.

BENEFITS OF HMIS AND AGENCY INFORMATION SHARING

Information you provide us can play an important role in our ability, and the ability of other Agencies, to continue to provide the services that you and others in our community are requesting.

Allowing us to share your real name, even in the absence of other information, results in a more accurate count of individuals and the services they use. The security system is designed to create a code that will protect your identity on the System. A more accurate count is important because it can help us and other Agencies:

- Better demonstrate the need for services and the specific types of assistance needed in our area.
- Obtain more money and other resources to provide services.
- Plan and deliver quality services to you and your family.
- Assist the Agency to improve its work with families and individuals who are homeless.
- Keep required statistics for state and federal funders (such as HUD).

RISKS IN SHARING INFORMATION

While the HMIS was designed to promote better services for those who are homeless or might become homelessness, there are risks that may lead some individuals to choose to do one or more of the following:

- Allow only your name, gender, year of birth, and partial social security number (optional) to be shared with all participating Agencies. All other information, including your date of birth,

full SS#, where you are being served and your particular situation, are kept confidential or shared with only select Agencies.

- Allow some statistical or demographic information to be shared with select other Agencies, but do not allow other more personal data such as health, mental health, drug/alcohol use history or domestic violence information to be shared.
- Close all information including identifying information from all sharing. Only the Agency that collects the information and System Administrative staff may see the information.

PRIVACY NOTICE AMENDMENTS: The policies covered under this Privacy Notice may be amended over time and those amendments may affect information obtained by the Agency before the date of the change. All amendments to the Privacy Notice must be consistent with the requirements of the Federal Standards that protect the privacy of clients and guide the HMIS implementation and operation.

Appendix J Sample

Privacy Policy

S A M P L E P O L I CY

DATE: June 25, 2014

SUBJECT: HMIS Privacy and Confidentiality

APPROVAL LEVEL: Agency Board of Directors

REASONS FOR POLICY:

1. To protect the privacy of Agency clients 2. To comply with applicable laws and regulations
3. To ensure fair information practices as to:
    a. Openness
    b. Accountability
    c. Collection limitations
    d. Purpose and use limitations
    e. Access and correction
    f. Data Quality
    g. Security

STATEMENT OF POLICY:

1) Compliance: Agency privacy practices will comply with all applicable laws governing the HMIS client privacy/confidentiality. Applicable standards include, but are not limited to the following:
    a) Federal Register Vol. 69, No. 146 (HMIS FR 4848-N-02) - Federal statute governing HMIS information.
    b) HIPAA - the Health Insurance Portability Act.
    c) 42 CFR Part 2. - Federal statute governing drug and alcohol treatment.
    d) CoC HMIS Policy and Procedures

Appendix J

Sample Privacy Policy

NOTE: HIPAA statutes are more restrictive than the HMIS FR 4848-N-02 standards and in cases where both apply, HIPAA over-rides the HMIS FR 4848-N-02 standards. In cases where an Agency already has a confidentiality policy designed around the HIPAA standards, that policy can be modified to include the HMIS data collection, or can be amended to create one set of standards for clients covered under HIPAA, and a second set of standards for those covered only under HMIS FR 4848-N-02.
Agencies should indicate in their Privacy Notice which standards apply to their situation.

2) Use of Information: PPI (protected personal information - information which can be used to identify a specific client) can be used only for the following purposes: a) To provide or coordinate services to a client.
   b) For functions related to payment or reimbursement for services.
   c) To carry out administrative functions such as legal, audit, personnel, planning, oversight and management functions.
   d) For creating de-personalized client identification for unduplicated counting.
   e) Where disclosure is required by law.
   f) To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
   g) To report abuse, neglect, or domestic violence as required or allowed by law.
   h) Contractual research where privacy conditions are met (including a written agreement).
   i) To report criminal activity on Agency premises.

NOTE: HMIS FR 4848-N-02 standards list items a-d above as allowable reasons for disclosing PPI but make provisions for additional uses to meet individual Agency obligations In some cases these uses (eI above) have additional conditions, and HMIS FR 4848-N-02 4.1.3 should be consulted if any of these optional items are to be included in an Agency's policy. It also states that "except for first party access to information and required disclosures for oversight and compliance auditing, all uses and disclosures are permissive and not mandatory."

3) Collection and Notification: Information will be collected only by fair and lawful means with the knowledge or consent of the client.
   a) PPI will be collected only for the purposes listed above.
   b) Clients will be made aware that personal information is being collected and recorded.
   c) A written sign will be posted in locations where PPI is collected. This written notice will read:

> "We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless and/ or at-risk persons, and to better understand the needs of homeless and/ or at-risk persons. We only collect information that we consider to be appropriate."
>
> "The collection and use of all personal information is guided by strict standards of confidentiality. Our Privacy Notice is posted. A copy of our Privacy Notice is available to all clients upon request."

   d) This sign will be explained in cases where the client is unable to read and/or understand it.

NOTE: Under HMIS FR 4848-N-02, Agencies are permitted to require a client to express consent to collect PPI verbally or in writing, however this is optional and not a requirement of the statute.

4) Data Quality: PPI data will be accurate, complete, timely, and relevant.
   a) All PPI collected will be relevant to the purposes for which it is to be used.
   b) Data will be entered in a consistent manner by authorized End Users.
   c) Data will be entered in as close to real-time data entry as possible.
   d) Measures will be developed to monitor data for accuracy and completeness and for the correction of errors.
      i) The Agency runs reports and queries at least monthly to help identify incomplete or inaccurate information.
      ii) The Agency monitors the correction of incomplete or inaccurate information. iii) By the 20th of the following month all monitoring reports will reflect corrected data.

e) Data quality is subject to routine audit by System Administrators who have administrative responsibilities for the database.

5) Privacy Notice, Purpose Specification and Use Limitations: The purposes for collecting PPI data, as well as its uses and disclosures, will be specified and limited.
   a) The purposes, uses, disclosures, policies, and practices relative to PPI data will be outlined in an Agency Privacy Notice.
   b) The Agency Privacy Notice will comply with all applicable regulatory and contractual limitations.
   c) The Agency Privacy Notice will be made available to Agency clients, or their representative, upon request and explained/interpreted as needed.
   d) Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.
   e) PPI will be used and disclosed only as specified in the Privacy Notice, and only for the purposes specified therein.
   f) Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the client.
   g) The Privacy Notice will be posted on the Agency web site.
   h) The Privacy Notice will reviewed and amended as needed.
   i) Amendments to, or revisions, of the Privacy Notice will address the retroactivity of any changes.
   j) Permanent documentation of all Privacy Notice amendments/revisions will be maintained.
   k) All access to, and editing of PPI data will be tracked by an automated audit trail, and will be monitored for violations use/disclosure limitations.

NOTE: Items above are required by HMIS FR 4848-N-02, and/or AL-501 HMIS policy, but Agencies can restrict and limit the use of PPI data further by requiring express client consent for various types of uses/disclosures, and/or by putting restriction or limits on various kinds of uses/disclosures.

6) Record Access and Correction: Provisions will be maintained for the access to, and corrections of, PPI records.
   a) Clients will be allowed to review their HMIS record within 5 working days of a request to do so.

b) During a client review of their record, an Agency staff person must be available to explain any entries the client does not understand.

c) The client may request to have their record corrected so that information is up-to-date and accurate to ensure fairness in its use.

d) When a correction is requested by a client, the request will be documented and the staff will make a corrective entry if the request is valid.

e) A client may be denied access to their personal information for the following reasons:

   i) Information is compiled in reasonable anticipation of litigation or comparable proceedings; ii) Information about another individual other than the Agency staff would be disclosed; and/or iii) Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

f) A client may be denied access to their personal information in the case of repeated or harassing requests for access or correction. However, if denied, documentation will be provided regarding the request and reason for denial to the individual and be made a part of the client's record.

g) A grievance process may be initiated if a client feels that their confidentiality rights have been violated, if access has been denied to their personal records, or if they have been put at personal risk, or harmed.

h) Any client grievances relative to the HMIS will be processed and resolved according to Agency grievance policy.

i) A copy of any client grievance relative to the HMIS data or other privacy/confidentiality issues and Agency response are forwarded to the CoC.

7) Accountability: Processes will be maintained to ensure that the privacy and confidentiality of client information is protected and staff is properly prepared and accountable to carry out Agency policies and procedure that govern the use of PPI data.

a) Grievances may be initiated through the Agency grievance process for considering questions or complaints regarding privacy and security policies and practices. All End Users of the HMIS must sign an End Users Agreement that specifies each staff person's obligations with regard to protecting the privacy of PPI and indicates that they have received a copy of the Agency's Privacy Notice and that they will comply with its guidelines.

b) All End User of the HMIS must complete formal Privacy Training.

c) A process will be maintained to document and verify completion of training requirements.
d) A process will be maintained to monitor and audit compliance with basic privacy requirements including, but not limited to, auditing clients entered against signed HMIS Releases.
e) A copy of any staff grievances initiated relative to privacy, confidentiality, or HMIS data will be forwarded to the CoC.

8) Sharing of Information: Client data may be shared with any Contributing HMIS Organization within the PromisSE implementation, unless entered by a provider with "closed" or partially "closed" visibility.
   a) Agency defaults within the HMIS System will be set to "open" unless otherwise requested by the Agency.
   b) A completed PromisSE HMIS Client Release of Information (ROI) Form is needed before information may be shared electronically. If the client refuses to have their information shared, their information is still entered into the HMIS but "closed" so that only that Agency and the System Administrators have access.
      i) The PromisSE HMIS release informs the client about what is shared and with whom it is shared.
   c) Clients will be informed about and understand the benefits, risks, and available alternatives to sharing their information prior to signing an ROI, and their decision to sign or not sign shall be voluntary.
   d) Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.
   e) All Client ROI forms related to the HMIS will be placed in a file to be located on premises and will be made available to the CoC for periodic audits.
   f) PromisSE ROI forms will be retained for a period of 7 years, while they are active, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
   g) No confidential/restricted information received from the HMIS will be shared with any organization or individual without proper written consent by the client, unless otherwise permitted by applicable regulations or laws.

h) Client information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence entered by Agencies with "closed" visibility shall not be shared with other participating Agencies without the client's written, informed consent. Sharing of "closed" information must also be planned and documented through a fully executed agreement between Agencies, as documented through an inter-Agency "closed" data sharing agreement. i) Sharing of "closed" information is not covered under the general PromisSE ROI.

ii) Once the client has provided written consent, and the involved Agencies have executed a sharing of "closed" information agreement for an individual client or household, a copy of those documents must be sent to the local HMIS System Administrator (SA), along with a ticket outlining the information to be shared and the receiving Agency. The SA will then "open" that information only to the receiving Agency.

i) If a client has previously given permission to share "closed" information with multiple Agencies and then chooses to revoke that permission with regard to one or more of these Agencies, the affected Agency/Agencies will be contacted accordingly, and those portions of the record, impacted by the revocation, will be "closed" from further sharing.

j) All client ROI forms will include an expiration date, and once a Client ROI expires, the Agency must contact the client in order to execute a new ROI. If the Agency is not able to contact the client, or if the client refuses to sign a new ROI, the Agency must notify the local SA within 48 hours so that the client record can be "closed".

9) System Security: System security provisions will apply to all Systems where PPI is stored: Agency networks, desktops, laptops, mini-computers, mainframes and servers. a) Password Access:

i) Only individuals who have completed Privacy and System Training may be given access to the HMIS through End User IDs and Passwords.

ii) Temporary/default passwords will be changed on first use.

iii) Access to PPI requires a End User name and password at least 8 characters long and using at least two numbers and/or special characters.

iv) End User Name and password may not be stored or displayed in any publicly accessible location

v) End Users must not be able to log onto more than one workstation or location at a time.

vi) Individuals with End User IDs and Passwords will not give or share assigned End User ID and Passwords to access the HMIS with any other organization, governmental entity, business, or individual.

b) Virus Protection and Firewalls:

i) Commercial virus protection software will be maintained to protect the HMIS from virus attack.

ii) Virus protection will include automated scanning of files as they are access by End Users.

iii) Virus Definitions will be updated regularly.

iv) All workstations will be protected by a firewall either through a workstation firewall or a server firewall.

c) Physical Access to Systems where HMIS Data is Stored

i) Computers stationed in public places must be secured when workstations are not in use and staff is not present.

ii) After a short period of time a password protected screen saver will be activated during time that the System is temporarily not in use.

iii) Staff must log out of the HMIS when leaving the workstation.

d) Stored Data Security and Disposal:

i) All HMIS data downloaded onto a data storage medium must be maintained and stored in a secure location.

ii) Data downloaded for purposes of statistical analysis will exclude PPI whenever possible.

iii) HMIS data downloaded onto a data storage medium must be disposed of by reformatting as opposed to erasing or deleting.

iv) A data storage medium will be reformatted a second time before the medium is reused or disposed of.

e) Hard Copy Security:

i) Any paper or other hard copy containing PPI that is either generated by or for the HMIS, including, but not limited to reports, data entry forms and signed consent forms will be secured.

ii) Agency staff will supervise at all times a hard copy with identifying information generated by or for the HMIS when the hard copy is in a public area. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.

iii) All written information pertaining to the End User name and password must not be stored or displayed in any publicly accessible location.

f) Remote Access to the HMIS:

i) All HMIS End Users are proscribed from using a computer that is available to the public or from accessing the System from a public location through an internet connection that is not secured. That is staff are not allowed to use Internet Cafes, Libraries, Airport Wi-Fi or other non-secure internet connections.

ii) Staff must use remote laptops or desktops that meet the same security requirements as those office HMIS workstations.

iii) Downloads from the HMIS may not include client PPI.

iv) Remote System access should be limited to situations in which it is imperative that the End User access the System outside of the normal office setting.

v) Remote System access should reflect the requirements of job responsibilities.

NOTE : Various important aspects of System security are the contracted responsibility of Bowman Systems and are therefore not covered in Agency policy. These involve procedures and protections that take place at the site of the central server and include data backup, disaster recovery, data encryption, binary storage requirements, physical storage security, public access controls, location authentication etc.

PROCEDURES:

NOTE: Procedures and roles relative to this policy should be defined in a procedure section. These will vary significantly from Agency to Agency but may include the following.

1. Participating Agencies may integrate the HMIS into the Agency's existing Privacy Notice. If the Agency does not have an existing Privacy Notice, Agencies may adopt the HMIS Privacy Notice Example in this manual or may use it as a model. The Privacy Notice must reflect the Agency's privacy policy.

2. Board approval of your Confidentiality/Privacy Policy is required. Copies of the Participation Agreement, the End User Agreement, Agency Administrator Agreement, Security Officer Agreement, and Inter-Agency “Closed” Data Sharing Agreement may be attachments to your Policy.

Universal Data Elements

Universal data elements are those which all HMIS participating continuum projects are required to complete. It is important to note that federal funding sources (programs) often require the projects they fund to maintain and report on additional data elements – identified as Program Specific elements. HMIS Universal Data Elements are elements required to be collected by all projects using the software as an HMIS. Projects funded by any one or more of the federal partners must collect the Universal Data Elements as must projects that are not funded by any federal partner (e.g. missions) but are entering data as part of the Continuum of Care's HMIS implementation.

Universal data elements enable the HMIS the ability to record unique, unduplicated client records, establish participation in a project within a date range, and identify clients who meet time criteria for chronic homelessness.

1 Name
2 Social Security Number
3 Date of Birth
4 Race
5 Ethnicity
6 Gender
7 Veteran Status
8 Disabling Condition
9 Residence Prior to Project Entry
10 Project Entry Date
11 Project Exit Date
12 Destination
13 Personal ID (HMIS Generated)
14 Household ID (HMIS Generated)
15 Relationship to Head of Household
16 Client Location Code (HMIS Generated)
17 Length of Time on Street, in an Emergency Shelter or Safe Haven

For more information and a full description of the Universal Data Elements, please reference the 2014 HUD Data Standards: HMIS Data Dictionary. **https://www.onecpd.info/resources/documents/HMIS-Data-Dictionary.pdf**

Program Management Information System of the Southeast PromisSE

Participation Agreement Between the Okaloosa Walton Homeless Continuum of Care and

_____

(Name of Continuum Designated HMIS Lead Agency)

Appendix L

HMIS Lead Partnership Agreement

This agreement is entered into on _____(mm/dd/yy) between the Okaloosa Walton Homeless Continuum of Care, designated as PromisSE's HMIS Lead Agency for FL-505, and the above stated Continuum designated Lead HMIS Agency hereafter known as "HMIS Lead," regarding access and use of the Program Management Information System, hereafter known as "PromisSE."

I. Introduction

The purpose of HMIS is to record and store client-level information about the numbers, characteristics and needs of persons who use homeless housing and supportive services, to produce an unduplicated count of homeless persons for each Continuum of Care in addition to the implementation; to understand the extent and nature of homelessness locally, regionally and nationally; and to understand patterns of service usage and measure the effectiveness of programs and systems of care.

PromisSE's goals are to:

- Improve coordinated care for, and services to, homeless and at-risk persons in the PromisSE service area,
- Provide a user-friendly and high quality automated records system that expedites client intake procedures, improves referral accuracy, increases case management and administrative tools, creates a tool to follow demographic trends and service utilization patterns of families and individuals either currently experiencing or at risk of experiencing homelessness, and supports the collection of quality information that can be used for program improvement and service-planning.
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD) and other funders as needed.

In compliance with all state and federal requirements regarding client/consumer confidentiality and data security, the PromisSE is designed to collect and deliver timely, credible, quality data about services and homeless persons or persons at risk for being homeless.

II. Okaloosa Walton Homeless Continuum of Care Responsibilities

1. Okaloosa Walton Homeless Continuum of Care, as PromisSE's HMIS Lead Agency for FL-505, will offer initial training for the HMIS Coordinator of each local HMIS Lead Agency, regarding the use of the HMIS compliant software used by PromisSE, so that the HMIS Coordinator will take responsibility for training end users within their Continuum. Okaloosa Walton Homeless Continuum of Care will provide notification of any Regional and other periodic training offered to HMIS Lead Agencies electronically at least two weeks in advance, barring extenuating circumstances.
2. Okaloosa Walton Homeless Continuum of Care, as PromisSE's HMIS Lead Agency for FL-505, will provide PromisSE software support and technical assistance (i.e., general trouble-shooting and assistance with standard report generation) to the HMIS Coordinator of each local HMIS Lead Agency. Access to this basic technical assistance will be available during normal business hours Monday through Friday (with the exclusion of holidays) and limited availability outside of normal business hours.
3. Okaloosa Walton Homeless Continuum of care will establish a fee structure for financing the software utilized by PromisSE, including an administrative fee.
4. Okaloosa Walton Homeless Continuum of Care will invoice participants in a timely manner.

5. Okaloosa Walton Homeless Continuum of Care will order user licenses at the request of the HMIS Coordinator of each local HMIS Lead Agency.

III. HMIS Lead Agency's Responsibilities

1. The HMIS Lead Agency agrees to maintain documentation of their annual designation as HMIS Lead Agency by their local Continuum of Care as established by HUD and notify Okaloosa Walton Homeless Continuum of Care, as PromisSE's HMIS Lead Agency, within 48 hours of any changes in this designation.
2. The HMIS Lead Agency agrees to participate as a member of the Program Management Information System of the Southeast's Steering Committee, the governing entity of PromisSE.
3. The HMIS Lead Agency agrees to designate and provide training for a Continuum System Administrator responsible for administering the PromisSE within the Continuum.
4. The HMIS Lead Agency agrees to support the HMIS Coordinator to ensure the Continuum Agencies who participate in PromisSE follow the basic standards as described in the PromisSE Policy and Procedure Manual and any Federal standards that supersede the Policies and Procedures.
5. The HMIS Lead Agency agrees to pay Okaloosa Walton Homeless Continuum of Care in full and on time for use of the PromisSE software and services associated with the HMIS software.
6. The HMIS Lead Agency agrees to make end user license and reporting license requests through Okaloosa Walton Homeless Continuum of Care.
7. The HMIS Lead Agency agrees to make Bowman requests through Okaloosa Walton Homeless Continuum of Care.

IV. Custody of Data

1. The HMIS Lead Agency and Okaloosa Walton Homeless Continuum of Care understand that the HMIS Lead Agency, agencies and Okaloosa Walton Homeless Continuum of Care as administrators, are custodians – NOT owners - of the data on behalf of the PromisSE participating agencies, or Contributing HMIS Organizations (CHOs).
2. In the event that PromisSE ceases to exist, Continuums will be notified and provided reasonable time to access and save client data on those served by their Contributing HMIS Organizations (CHOs), as well as statistical and frequency data from the entire system. Thereafter, the information collected by the centralized server will be purged or appropriately stored.
3. In the event that Okaloosa Walton Homeless Continuum of Care ceases to exist, the custodianship of the data within PromisSE will be transferred to the agency designated as the new PromisSE HMIS Lead Agency by the PromisSE Steering Committee for continuing administration, and all PromisSE Continuums will be informed in a timely manner.
4. In the event that the HMIS Lead Agency ceases to exist, the custodianship of the data within PromisSE will be transferred to the either the local Continuum of Care or the organization designated by the local Continuum of Care as the new HMIS Lead Agency for continuing administration.

V. Hold Harmless

1. Okaloosa Walton Homeless Continuum of Care makes no warranties, expressed or implied. The HMIS Lead Agency, at all times, will indemnify and hold Okaloosa Walton Homeless Continuum of Care harmless from any damages, liabilities, claims, and expenses that may be claimed against the HMIS Lead; or for injuries or damages to the HMIS Lead Agency or another party arising from participation in the PromisSE; or arising from any acts, omissions, neglect, or fault of the HMIS Lead Agency or its agents, employees, licensees, or clients; or arising from the HMIS Lead Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This HMIS Lead Agency will also hold Okaloosa Walton Homeless Continuum of Care harmless for loss or damage resulting in the loss of data due to delays,

non-deliveries, mis-deliveries, or service interruption caused by the chosen software vendor for PromisSE by the HMIS Lead Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. Okaloosa Walton Homeless Continuum of Care shall not be liable to the HMIS Lead Agency for damages, losses, or injuries to the HMIS Lead Agency or another party other than if such is the result of gross negligence or willful misconduct of Okaloosa Walton Homeless Continuum of Care. Okaloosa Walton Homeless Continuum of Care agrees to hold the HMIS Lead Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of Okaloosa Walton Homeless Continuum of Care.

2. It is the responsibility of the HMIS Lead Agency to ensure that each participating Agency within the Continuum maintain compliance with all PromisSE Policies and Procedures in addition to any required by Federal standards.

VI. Terms and Conditions

1. The HMIS Lead Agency shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of Okaloosa Walton Homeless Continuum of Care.
2. This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term occurs if allegations or actual incidences arise regarding possible or actual breeches of this agreement. Should such situations arise, the Okaloosa Walton Homeless Continuum of Care PromisSE System Administrator may immediately suspend access to PromisSE until the allegations are resolved in order to protect the integrity of the system.
3. This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.

IN WITNESS WHEREOF, the parties have entered into this Agreement:

Okaloosa Walton Homeless Continuum of Care
207 Hospital Drive NE, Suite B.
Fort Walton Beach, FL 32548

_____	_____
OWHCoC Telephone Number	HMIS Lead Agency Telephone Number
_____	_____
OWHCoC Representative Printed Name	HMIS Lead Agency Representative Printed Name
_____	_____
OWHCoC Representative Title	HMIS Lead Agency Representative Title
_____	_____
OWHCoC Representative Signature	HMIS Lead Agency Representative Signature
_____/_____/_____	_____/_____/_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix L

HMIS Lead Partnership Agreement

Program Management Information System of the Southeast Lead Agency for FL 505
Okaloosa Walton Homeless Continuum of Care

ASSURANCE

_____ (Name of HMIS Lead) assures that the following fully executed documents will be on file and available for review.

- Documentation of the designation of the HMIS Lead Agency's by the local Continuum of Care.
- The HMIS Lead Agency's Board Approved Confidentiality Policy.
- The HMIS Lead Agency's Official Privacy Notice for PromisSE clients.
- Documentation authenticating completion of required training for all PromisSE System Users in the Continuum.
- A fully executed User Agreement for all PromisSE End Users in the Continuum.
- A fully executed participation agreement for all PromisSE Contributing HMIS Organizations (CHOs)
- A current HMIS Lead Agency PromisSE Policy and Procedure Manual.
- The HMIS Lead Agency's Conflict of Interest Policy.
- The HMIS Lead Agency's Whistleblower Policy.

By: _____

Title: _____

Signature: _____

Date: _____

Appendix M

CoC System Administrator Agreement

CoC System Administrator Agreement

Name:_____
CoC Name:_____

All HMIS participating CoCs must designate and staff one HMIS System Administrator. System Administrator requirements and responsibilities include, but are not limited to, the following:

- Has completed, at minimum, System Administrator training.
- Ensure that all Agency users have signed End User Agreement documents on file.
- Ensure that all Users complete an annual End User Certification Test, which includes Privacy and Security training.
- Ensure that all Users have completed workflow training and related updates, and have documentation of training.
- Ensure that the CoC is in compliance with the CoC Data Security standards.
- Ensure that the CoC is in compliance with the PromisSE HMIS Policies and Procedures.
- Ensure that all Users have submitted a criminal background check.

The original System Administrator Agreement shall be kept on file at the CoC. Forms completed by individuals no longer employed by the CoC shall be kept on file for a minimum of five years.

Okaloosa Walton Homeless Continuum of Care makes no warranties, expressed or implied. The CoC, at all times, will indemnify and hold the Okaloosa Walton Homeless Continuum of Care harmless from any damages, liabilities, claims, and expenses that may be claimed against the CoC; or for injuries or damages to the CoC or another party arising from participation in the ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the CoC's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This CoC will also hold Okaloosa Walton Homeless Continuum of Care harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the CoC's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. Okaloosa Walton Homeless Continuum of Care shall not be liable to the CoC for damages, losses, or injuries to the CoC or another party other than if such is the result of gross negligence or willful misconduct of Okaloosa Walton Homeless Continuum of Care. Okaloosa Walton Homeless Continuum of Care agrees to hold the CoC harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of Okaloosa Walton Homeless Continuum of Care.

This agreement is in effect for a period of one (1) year after date of signing. Failure to comply with the provisions of this System Administrator Agreement is grounds for immediate termination of access. Your signature below indicates your agreement to comply with this System Administrator Agreement.

_____	_____
CoC Official Printed Name	Employee Printed Name
_____	_____
CoC Official Signature	Employee Signature
_____/_____/_____	_____/_____/_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix N

CoC System Security Officer Agreement

CoC System Security Officer Agreement

Name:_____

Agency Name:_____

All HMIS participating CoCs must designate and staff one CoC HMIS Security Officer. Security Officer requirements and responsibilities include, but are not limited to, the following:

- Ensures that all staff using the system complete annual privacy and security training. Training must be provided by the CoC designated trainers and be based on the CoC Privacy and Security standards.

- Conducts an annual security review of the CoC that includes reviewing compliance with the Privacy and Security sections of the PromisSE Homeless Management Information System (HMIS) Operating Policy and Procedure. The CoC must document the findings of the review on the Privacy and Security Checklist and submit the findings to the Lead HMIS System Administrator no later than December 31st of each year.

- Notifies the local Lead Agency System Administrator when a System Administrator leaves the organization or revision of the user's access level is needed because of a change in job responsibilities. The notification must be made within 48 hours of the change.

- Reports any security or privacy incidents to the local Lead HMIS System Administrator for the CoC Jurisdiction. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the CoC. A Corrective Action Plan will be implemented. Components of the Plan must include at minimum supervision and retraining. It may also include removal of HMIS license, client notification if a breach has occurred, and any appropriate legal action.

The original Security Officer Agreement shall be kept on file at the CoC. Forms completed by individuals no longer employed by the Agency shall be kept on file for a minimum of five years.

Okaloosa Walton Homeless Continuum of Care makes no warranties, expressed or implied. The CoC, at all times, will indemnify and hold the Okaloosa Walton Homeless Continuum of Care harmless from any damages, liabilities, claims, and expenses that may be claimed against the CoC; or for injuries or damages to the CoC or another party arising from participation in the ***PromisSE***; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or clients; or arising from the CoC's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This CoC will also hold Okaloosa Walton Homeless Continuum of Care harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the CoC's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. Okaloosa Walton Homeless Continuum of Care shall not be liable to the CoC for damages, losses, or injuries to the CoC or another party other than if such is the result of gross negligence or willful misconduct of Okaloosa Walton Homeless Continuum of Care. Okaloosa Walton Homeless Continuum of Care agrees to hold the CoC harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of Okaloosa Walton Homeless Continuum of Care.

This agreement is in effect for a period of one (1) year after date of signing. Failure to comply with the provisions of this System Security Officer Agreement is grounds for immediate termination of access. Your signature below indicates your agreement to comply with this System Security Officer Agreement.

_____	_____
Agency Official Printed Name	Employee Printed Name
_____	_____
Agency Official Signature	Employee Signature
_____/_____/_____	_____/_____/_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix O

CoC Agency Audit Checklist

____ Has completed and submitted Policies and Procedures Compliance Checklist

____ Has completed annual Privacy and Security Checklist

____ All End Users have executed End User Agreement

____ HUD Public Notice is posted and visible to clients

____ Has HMIS Privacy Notice and is available to clients

____ Has HMIS Privacy Policy which details the procedures of the Privacy Notice

____ HMIS Privacy Policy includes a remote access plan

____ Hard copy data is secure

____ HMIS workstations are password protected

____ HMIS workstations have time scheduled locked settings

____ All clients are entered into the System within 48 hours of intake

____ All End Users have received a copy of the HUD Data Elements

____ Staff members have been trained on the HUD definition of homelessness and understand the priority of homelessness documentation

____ Agency has process to ensure clients name is spelled properly and DOB is accurate

____ End Users are updated client information as required for program type through Interim Reviews and Follow Ups

____ Agency Admins or assigned staff are running monthly data quality reports and making corrective action in accordance with the requirements of the CoC Policies and Procedures

____ All End Users have had at least general ClientPoint training

Agency HMIS Performance Evaluation

Date: _____

Project: _____

Program manager: _____

Score the Project on each of the following performance measures on a scale of 0-4. Where 4 = Far exceeds expectation, 3= Exceeds expectation, 2= Expected performance, 1 = Marginal performance, 0=Unsatisfactory.

A. Timeliness _____

B. Completeness _____

C. Accuracy _____

D. Consistency _____

E. Utilization of PromisSE (HMIS) Modules _____

Overall Data Quality Score (sum of items A-E) _____

Does the project meet HUD data quality standards? Yes No

Comments:

_____ _____

Signature of Reviewer Date