VESTA®

Policies & Procedures

Updated June 2015

Contents

Introduction

The policies and proceedures outlined in this manual are those that have been developed by The Partnership Center, Ltd. (PCL) in cooperation with our local VESTA Advisory Committee. PCL is the developer and manager of VESTA® – the Virtual Electronic Service Tracking Assistant software, designed to measure performance, track accomplishments, report to funders, manage services, and facilitate integrated service approaches. We work with federal agencies, funders, and community service organizations that plan, fund, or provide housing and services to persons experiencing homelessness and/or low-income persons.

In 1999 PCL created a local Homeless Management Information(HMIS) Advisory Committee to create a mechanism for community feedback into the design, creation, policies and procedures of VESTA, the software selected by the Cincinnati/Hamilton County Continuum of Care for the Homeless's HMIS. Over the years as VESTA has grown in use across the Greater Cincinnati community so also has the Advisory Board grown to now not only reflect the needs and issues of HMIS, but also of all of the other community users of the system.

Questions regarding VESTA or the contents of this manual should be directed to:

The Partnership Center, Ltd.
2134 Alpine Place
Cincinnati, OH 45206
www.partnershipcenter.net
phone: 513-891-4016 x 336
email: techsupport@partnershipcenter.net

General Participation Policies and Procedures

Data Ownership

Policy: All data entered into VESTA is owned by the Agency entering the data. Individual client level data about all persons served by the Agency, whether in a homeless project or other Agency project, may be entered into VESTA.

Procedure:

- Client-level identifying information will not be released by The Partnership Center, Ltd. (PCL) for any reasons other than those required by law.
- As a community database, VESTA enables different Agencies to record information about clients and services within a single common software system and to create partnership/data-sharing agreements with other Agencies as the Agency determines appropriate.
- As a community database, basic demographic information for any client, who has signed a consent form, is shared with other VESTA Users who are also serving the same client, once the client has entered their project. Project-specific data will not be shared with another Agency without the expressed consent of this Agency in the form of a signed Partnership Agreement.

Agency Participation Expectations

Policy: The Agency agrees to use the VESTA software as part of the community's effort to provide accurate data on homelessness, for their own record keeping of all client level data, and as a reporting tool for all reports necessary for the Agency and its funders.

Procedure: The Agency agrees to the following terms for using VESTA in accordance with federal, local HMIS rules, and guidance provided by VESTA clients (such as United Way of Greater Cincinnati):

- The Agency commits to entering truthful, accurate, complete, and timely information to the best of their ability on all clients receiving homeless and/or emergency assistance services.
- The Agency may not use VESTA system participation, or data, as a reason to deny outreach, shelter, housing, or emergency assistance services to a client. Emergency assistance agencies deny specific funding for emergency assistance to a client for reasons specified as a condition of receiving the funds, (such as EFSP funds) or as a result of agreements/best practices defined through the EA Learning Circle, (i.e., not providing stabilization services to a client because he or she is currently being served by another project in stabilization).
- The Agency may customize their data collection, including additional client-level information as needed by their project(s), but must collect all HMIS-required data fields as indicated in the US Department of Housing and Urban Development (HUD) HMIS Data Standards (identified in VESTA as required fields), and/or data required by the appropriate funder.
- The Agency agrees to allow clients to view their own HMIS / services data and request changes or corrections to their data.
- The Agency agrees that the data entered into VESTA will be monitored by PCL. PCL will merge duplicate client records on a regular basis. There will be no data monitoring on any custom fields developed by Agencies for their own use or for any projects enrolled in VESTA outside the Continuum of Care (CoC) and/ or United Way

administered funding.

- The Agency agrees that public reporting in aggregate either collectively, by program, or by project type for all CoC projects enrolled in VESTA as part of HMIS and/or projects funded by United Way administered funds may be released as needed by the funder.
- The Agency agrees to abide by all VESTA policies and procedures as approved and adopted by the VESTA Advisory Board. These include: confidentiality, client consent, and data entry requirements. Agencies also agree to assure that all employees and agents comply with these policies.
- Specific to HMIS projects: Consistent with Strategies to End Homelessness' agreement with the U.S. Department of Housing and Urban Development, all CoC Agencies may view and print Homeless Certification forms generated by HMIS as a way to document clients' eligibility for services.

Data Entry

Policy: VESTA continues to be designed for live data entry; as a result, all Agencies participating in VESTA are encouraged to enter data into VESTA in a timely manner. For HMIS projects, specific timeliness policies are required and HMIS participation may not be used to deny services.

Procedure:

- One hundred percent (100%) of all CoC homeless certified clients are to be entered into the system, detailing basic data, services and special needs data based on the most recent data standards - see HUD Exchange for details and project requirements.
- Real Time Data Entry is encouraged. However, in cases where real time cannot be accomplished the following timeframes are requied:
  - Residential Projects: All data required to be collected at project entry is to be entered into the HMIS system within **two working days** of a residential project entry. Residential projects include: emergency shelter, transitional housing, and all types of permanent housing including rapid re-housing and permanent supportive housing. In accordance with HUD policy all residential projects where persons reside for a year or longer must do an annual assessment within the 30 day before or 30 day after the client's anniversary of project entry each year.
  - Emergency Assistance, Service Only, and Stabilization Projects: All intake data is required to be collected at project entry is to be entered into the HMIS system within **two working days** of a residential project entry. All data documenting specific shared services, such as holiday basket/ gift sign ups, should generally be recorded at the time of service to prevent duplication of these services.
  - Street Outreach Progects: Limited basic demographic data (race, gender, and a unique identifier) is to be entered into the HMIS system within two working days of the first substantial outreach encounter.
  - Exit Data: All data required to be collected at project exit data is to be entered into the HMIS system within **five working days** of the client exiting a housing stay or receiving a service.

The Role of the Partnership Center, Ltd.

Management of VESTA

Policy: PCL assumes the following expectations as the administer and owner of VESTA. Annual licensing fees for VESTA are provided by Strategies to End Homelessness, under a grant from the U.S. Department of Housing and Urban Development specifically for HMIS and from the United Way of Greater Cincinnati. The licensing fee provides the Agency with:

VESTA Management:

1. Maintain VESTA and VESTA servers to ensure daily operation with minimal outages.
2. Software updates - no less than three times per year.
3. Code documentation and deployment record keeping: Ensure the VESTA code is well documented and

maintain records of changes made at each deployment.
4. Ensure VESTA software is fully compliance with all HMIS Data and Technical standards and United Way requirements.
5. Report functionality for Funder Reports including: HMIS Reports for HUD, HHS, and VA programs; United Way Reports for EA, Emergency Food and Shelter Board, City of Cincinnati General Fund, and Basic Demographic.
6. Report functionality for Universal reports including: Active Client List, Bed night list, Export via Access and CSV.
7. Oversight of the day-to-day administration of all contracts/ jobs with PCL for the use of VESTA.
8. Record keeping: ensure all Agencies have signed an Agency agreement, ensure all sharing agreements are documented and signed prior to sharing, and maintain current User agreements for all active Users.
9. Organize and manage a VESTA Advisory Board oversight of Emergency Assistance and HMIS implementation.

HMIS Lead Agency Role Participation Expectations

Definition: A Lead Agency is an organization designated by a CoC to operate the CoC's HMIS. The Cincinnati/Hamilton County Continuum of Care for the Homeless designates Strategies to End Homelessness (STEH), as the HMIS Lead Agency. STEH has contracted with The Partnership Center, Ltd., the software vendor for VESTA, the following scope of work and roles as articulated in the following*:

**Please note, work or roles listed below are in addition to the work and roles provided in the previous section – Management of VESTA.*

HMIS Project Management:

1. Oversight of the day-to-day administration of the HMIS project.
2. Ensure all Community Housing Organization (CHO's) designated by STEH and the HMIS Advisory Board have signed Agency Agreements to utilize VESTA as their HMIS and monitor compliance with the agreement.
3. Maintain an active list of all CHO's participating in VESTA as part of the community's HMIS and enter into VESTA the following project descriptor data elements on each project:
    a. Organization Identifier
    b. Organization Name
    c. Project Identifier
    d. Project Name
    e. Direct Service Code
    f. Site Information
    g. Continuum of Care Number
    h. Project Type Code
    i. Annual and Grant Based Bed and Unit Inventory Information
    j. Target Population Data
    k. Method for tracking Residential Project Occupancy
4. Produce annual e-HIC as specified by HUD in order to generate annual Bed and Unit Inventory Information.
5. Maintain all User Agreements, assign User levels, and monitor agreement compliance.
6. Provide staff support to the VESTA Advisory Board – HMIS Sub group.
7. Provide documentation required by HUD for the Annual CoC Grant- HMIS section.

VESTA User Training:

1. HELP Desk – User Support by telephone and email during regular business hours, (Monday - Friday from 9AM – 5PM).
2. Provide individual or small group training for all new Users of HMIS and United Way projects.
3. Free classroom training on basic and advanced database use skills.
4. Provide training on new features of VESTA as needed for HMIS Data Standards compliance.

5. Development of training materials and methods as may be necessary to keep Users at the highest possible proficiency level.

HMIS User Support:

1. Research and respond to CHO or User questions, problems and inquiries in a timely fashion.
2. Provide support services to organizations to customize their data for implementation of VESTA and/or to support all funding and reporting requirements of the project.
3. Utilize newsletters, email communication, groups, etc. to maintain User engagement and proficiency.

HMIS Data Quality:

At least weekly, monitor error reports on all Users and proactively address errors for Users above approved tolerance levels.

1. At least quarterly, perform unduplication of all records.
2. At least annually, monitor CHO projects for data quality & outcome performance as measured on their APR.
3. Lock Agency data within 90 days of completion of the grant operating year.

HMIS Data Reporting:

1. Annually, or as required by HUD or the CoC, produce the Electronic Housing Inventory Chart (e-HIC).
2. Annually, or as required by HUD, produce the Annual Homeless Assessment Report (AHAR) and electronically submit it as required.
3. Provide documentation required by HUD for the Annual CoC grant application on HMIS data.
4. Produce the annual HMIS Data Report.

Operational Policies and Procedures

Chronically Homeless Individuals Project (CHIP)

Policy: Chronically Homeless Individual's Program (CHIP) is the method used to identify, on a long-term basis, those single individuals (or heads of household) who are chronically homeless and came into the system through an Outreach or Emergency Shelter project.

Procedure:

The VESTA Advisory Board authorized an effort to track accomplishments with the chronically homeless and to permanently mark persons entering the system through outreach or emergency shelter that meet the following:

- They have entered the system as unaccompanied, single individuals; or as a chronically homeless head of household for a family.
- They are recognized as having a disabling condition.
- They have been self-identified as being homeless for longer than 1 year or more than 4 times in 3 years.

Once an outreach client or shelter resident meets the three indicators they will be identified in VESTA as a CHIP client. CHIP permanently flags clients. This Permanent flag remains with the client regardless of their future intakes at any other projects.

Client Consent

Policy: It is VESTA and HMIS Policy that all clients are provided with a client consent form (CCF) as authorized by the HMIS Lead Agency and VESTA Advisory Board to inform them that, if consent is granted, their personal identifying information will be shared within the VESTA community database. Withholding consent does not allow a client to keep the Agency that is housing/serving them from entering their data into VESTA. Consent only governs the sharing of that data within the wider community database.

Procedure:

Timing:

1. Clients should be informed about the VESTA consent process, and provided the opportunity to sign a CCF the first time they are entering in a housing (emergency shelter, transitional housing, permanent housing), service, or other project that utilizes VESTA.
2. VESTA consents are valid across the entirety of the database—once a client signs a consent, it allows their basic personal information to be seen across the system.
3. During each project intake, VESTA Users will have the option to utilize an existing consent (if one exits), generate a new client consent form, or renew an expired/expiring consent.

Signature:

1. VESTA allows for consent forms to be signed and stored electronically within the database. Agencies may elect to print and maintain physical copies of signed consents, but all consents must be recorded within VESTA to allow client data to be seen outside the original entering Agency.
2. All adult members of households should be provided the opportunity to consent. Consent for data entry/updating for minors will be provided for in the language of the parent/guardian's CCF.
3. Agency data entry/updating permission applies only to clients currently receiving services or housing.

Renewal:

1. All consent forms expire after three years. If a client is still in residence, a new consent form must be offered to them at the time of lease renewal or annual assessment.

Revoking Consent:

1. Consent may be revoked by a client at any time. [Revoking consent means that all client data will no longer be viewable to any other outside project or Agency. Data will still be recorded in VESTA and will still be viewable by the provider Agency.]

Unattainable Consent:

1. If a CCF cannot be obtained, the Agency shall enter client data as non-releasable data to be viewed by only that project for aggregate reporting purposes.
2. A client's decision to not sign a CCF may not be used as a reason to deny them housing or services.

Individual client information sharing:

1. A CCF does not authorize the Agency to release information about a client from the database. The Agency's own Agreement and release form and process must still be used prior to information sharing.

Client Grievance

Policy: Client has the right to appeal his or her individual issues related to their HMIS data to the entering Agency.

Procedure: If a client has a complaint related to HMIS, they may file a grievance in accordance with the Agency's established grievance policy. In the absence of an established Agency grievance process, clients may address their concerns by the following progression:

1. Case worker
2. Case worker's supervisor
3. Executive Director of the Agency

Client Notification/ VESTA Workstation Requirements

Policy: Because of the confidential nature of data stored within VESTA and its use as a community database application, the system must be accessed from a secured and semi-private location. Computers located in public areas will not be given access to VESTA. All computer work stations entering HMIS data will be identified with the official HMIS Poster. Work stations entering VESTA data must be identified with the "VESTA used here" sticker.

A written notice of the assumed functions of VESTA must be posted and/or given to each client so they are aware of the potential use of their data that is given, as a part of receiving services from the project. No consent is required. All clients have the right to refuse to participate.

Procedure:

- For HMIS projects: Notification as an HMIS work station must be prominently displayed at each computer work station where HMIS data is entered or in a prominent location in a service area.
- For all other projects: Notification of "VESTA used here" must be prominently displayed at the work station or on the primary entrance of the project.
- If the work station is not accessible to customers, an official Cincinnati/Hamilton County HMIS Poster must be displayed.

Data Access/Sharing

Policy: Client confidentiality and privacy are core values of the HMIS system. Data may only be shared pursuant to signed agreements between Agencies. Full data sharing among Agencies will only be allowed with a signed partnership agreement spelling out details, services, terms, and participating Agencies. Agency data entry/updating permission applies only to clients currently receiving services or housing.

Procedure: VESTA identifies the following data sharing levels

- Level 1 – Indicates data that will be shared among VESTA Users with projects other than the intake project as long as a consent form has been signed and indicated in VESTA.
- Level 2 – Indicates data that will be shared pursuant to the execution of a Partnership Data Sharing Agreement signed by all partner Agencies.
- Level 3 – Indicates data that will never be shared, regardless of consent or partnership agreement.

Data Entry/Editing

Policy: The data in VESTA is the property and the responsibility of the project that entered it.

Procedure: PCL will not alter data, except under the following circumstances:

1. Agency data may be altered by PCL Staff in the course of routine system maintenance, such as the merging of duplicate client records. (See Unduplication Approach for additional details on record merging)
   Example: Record A shows JOE WILLIAMS with a date of birth of 1/1/1925. Record B shows Joseph Williams with a date of birth of 1/1/1925. Both records show the same SSN. In this case JOE WILLIAMS will be merged in to Joseph Williams's record.
2. Agency data may be altered by PCL Staff in the event that the data as entered by the Agency prevents accurate reporting or functioning. In most cases, VESTA prevents the entry of such data, but there are exceptions.
   Example: A User enters '$400.00' as an income amount. The dollar sign prevents VESTA from recognizing the data as a number; it is not possible to report on the data in the field. PCL Staff will remove the dollar sign.
3. Agency data may be altered by PCL Staff in the event that data collection and/or reporting requirements

change such as data as previously entered is non-compliant or non-reportable under new requirements.
Example: HUD changes the list of valid prior living situations. PCL Staff will 'translate' the existing data en masse to the best possible match within the new list.

- Minor edits and alterations made in the course of routine system and/or data maintenance, such as those described in paragraphs one and two above, are pre-authorized by the VESTA Advisory Board. Data alteration en masse, such as that described in paragraph three above, must be a type that could only reasonably be done as a central administrative function rather than by individual Agencies; it should be undertaken only in coordination with the VESTA Advisory Board and with advanced notice to Agencies. If possible, Agencies should have the option to receive a copy of their original data for reference purposes.
- These categories of authorization reflect a response to a system-level problem, not an Agency problem. If the threat to data is not a system threat but rather a problem with the records of individual Agencies, then it is the responsibility of each Agency to clean its data. While VESTA Support Staff should continue to assist individual Users with any appropriate problem, this document is not meant to relieve any Agency of responsibility for the correctness of its data. VESTA Support Staff may help a User to fix his or her data for a client, but VESTA Support Staff cannot be responsible for an Agency's entire record keeping and data entry requirements.

HMIS Data Standards/Elements

Policy: An HMIS system must implement, at a minimum, the HUD HMIS Data Standards within one year of each version's release. HMIS Data Standards include fields and responses for each of the provider project descriptor data elements, universal data elements, provider project-specific data elements, and metadata elements.

Procedure:

- As the National HMIS Research Lab, VESTA is required to implement newer versions of the HMIS Data standards in advance of their general implementation.
- VESTA complies with all HUD reporting requirements associated with HMIS Data Standards data in accordance with the most current version.
- When fields/responses are modified/aggregated as part of a new HMIS Standards release, data is migrated to the appropriate field/response to ensure that data integrity is maintain historically.
- While all projects in VESTA are required to collect those HMIS Standard elements associated with their project type, VESTA also allows each project to customize what other data and reporting they want for their own project.

Data Release

Policy: Data contained within the Homeless Management Information System (HMIS) is intended to be utilized at the Agency level for project monitoring, reporting, and planning and at the community level for government funding accountability, to increase the general population's accurate understanding of homelessness and to inform policy and decision making around homeless issues/funding.

Procedure:
System-wide Level:

- Each Agency owns the client data for housing and/or services provided by them.
- Agencies are encouraged to use their own HMIS data for public relations, reporting, and funding as long as client confidentiality is maintained.
- Community-wide aggregate HMIS homeless data (not Agency specific) will be published annually by PCL. These reports will be raw point-in-time data. An Agency may use any and all summary data published in the annual VESTA Community Data Report.

- Any researcher interested in accessing the data, after ascertaining from the Partnership Center the specific kinds of data they are interested in and the format required, must submit, in writing, a request to the VESTA Advisory Board. No identified data will be released by PCL for research purposes.
- STEH, on behalf of Cincinnati/ Hamilton County Continuum of Care for the Homeless (CoC), may use HMIS data for planning, reporting, and grant writing purposes. The CoC may reconcile and release aggregate data to the City of Cincinnati and Hamilton County without VESTA Advisory Board review for reporting purposes including: Consolidated Plan development/reporting, HUD reporting, ESG reporting, IDIS, etc.

The HMIS Lead Agency, STEH, may release aggregate data for the purpose of community-wide reporting as required (e.g. Annual Homeless Assessment Report). Neither PCL nor STEH will release any project-specific or client-level data without the consent of the Agency and/or individual except as required by law.

Vesta Advisory Board Role

Purpose: To guide the on-going planning, development, and implementation of a community-wide Homeless Management Information System (HMIS) for the Cincinnati-Hamilton County Continuum of Care for the homeless and VESTA as a community database for the region and other social services.

Mandate: The VESTA Advisory Board HMIS Committee mandate is to oversee the HMIS implementation and usage throughout the CoC. It also serves in an advisory capacity to The Partnership Center.

Work of the HMIS Committee:

- Ensure that the community's HMIS is able to fulfill all functions required by HUD for an HMIS system including but not limited to: implementation of new/ updated data standards, Annual progress Reporting, Annual Homeless Assessment Reporting, etc.
- Monitor/improve/revise security and confidentiality protocols.
- Develop and oversee all local CoC HMIS Policies and Procedures.
- Represent Users' interests regarding use of VESTA as the community's HMIS.
- Review, recommend, and initiate action on significant HMIS issues uncovered during project monitoring.
- Review and recommend VESTA changes/upgrades as they relate to its use as the community's HMIS.
- Respond to any community grievances (Agencies, projects, or Users) regarding HMIS.
- Establish the annual fee schedule for HMIS Agencies.
- Review/approve all research, data warehousing, and data integration project requests.

Asset Management: The VESTA Advisory Board HMIS Committee will make recommendations to the HMIS Lead Agency, currently STEH, regarding asset disbursement, should the need arise.

Work of the EA Committee: The VESTA Advisory Board EA Committee oversees and guides the implementation and growth of EA implementation in VESTA. This committee works closely with the EA Learning Circle, led by United Way of Greater Cincinnati.

Meeting: The VESTA Advisory Board meets on a rotating schedule, with Committees meeting every other month and the full Board meeting quarterly. Additional committees may be developed as necessary and may consult with additional Agencies and resources in the community. VESTA Advisory Board meeting minutes will be filed at PCL.

Term and Structure: The VESTA Advisory Board will serve as advisors to PCL and STEH. Membership on the committee will be reviewed annually and should have at least one representative of each of the following project types: emergency shelter, transitional housing, permanent supportive housing, and street outreach. The chair of the committee is elected annually and may serve no more than two consecutive terms. The Executive Director of the STEH (or their designee) is an ex-officio member of the HMIS sub-committee and a staff of United Way of Greater Cincinnati will is an ex-officio member of the EA sub-committee. PCL will staff the sub-committees.

HMIS Monitoring

Policy: To ensure that Agencies are maintaining high quality data (specifically with regard to HMIS data standards and HUD measured outcomes), each project in VESTA will be monitored by PCL Staff on at least an annual basis.

Procedure:

1. PCL will generate a monitoring report covering a one-year period that corresponds to the project grant year being monitored or one year from the end of the previous month.
   - CoC projects will be monitored in the month following the close of their grant operating year.
   - ESG projects will be monitored annually in accordance with their annual reporting requirements.
   - Projects which provide homeless certification but do not have a HUD grant will be monitored annually in a month agreed upon between the project and PCL.
   - All other grant projects will be monitored in accordance with their grant terms.
   - Notes/exceptions:
     a. Projects that have multiple grants will only be required to be monitored once annually at the close of the first operating year of the calendar year. (Additional monitoring on a grant-by-grant basis can be arranged by mutual agreement.)
     b. Projects that have ESG funding and CoC funding will be monitored on the CoC grant schedule.
2. PCL will review the monitoring report, making appropriate notes in a monitoring template. (Template outlines data retrieved in each area and any comments related to each item listed above.)
3. The monitoring report and template will be emailed to the supervisor of the project being monitored and any other key staff the Agency has identified to participate. The email will contain information on what elements the monitoring has identified as issues or areas of concern and are further detailed in the monitoring report. If the monitoring findings identify multiple significant issues, an on-site monitoring will be scheduled. Project supervisors will be asked to have each issue addressed in one of the following ways:
   - data review and correction as necessary,
   - scheduling follow up training for a User, and/or
   - documentation of a new process/policy/procedure for future correction of the issue going forward.

<u>Items to be monitored include:</u>

1. VESTA Front End data accuracy
2. HMIS issues:
   - Data quality based on all APR required fields
   - Data quality of Health Foundation fields
   - Error alerts
   - Client consent (# of clients with signed consent forms)
   - Timeliness of data entry (intake and exit)
   - Average time lapse between days of activity to days of data entry for intake/exit data entry
3. Grant related issues:
   - # of persons without an auto generated homeless certificate
   - Average daily capacity as compared to housing inventory
   - Recidivism rate
4. Outcomes:
   - Income
   - Clients with a loss of income and benefits over the stay
   - Annual recertification of income for all TH and PSH projects
5. Housing
   - Exit destination as compared to recidivism

<u>Monitoring Close Out</u>

1. Corrective action is to be documented on the monitoring template by the project and return to PCL within 30 days.

2. On the 31st day (or the workday thereafter) PCL will review the areas of concern in VESTA to assure all have been corrected or addressed.
3. Follow up action will be taken as necessary according to the monitoring response matrix below.
4. Project data is locked.

Response 1

- A letter from PCL will be mailed to the Executive Director (ED) of the Agency, copied to the project supervisor, indicating the positive monitoring outcome.
- Strategies to End Homelessness will be notified of positive outcome via email.

Response 2

- A letter from PCL will be mailed to the ED of the Agency, copied to the project supervisor indicating the monitoring outcome, the issue(s) addressed, and the action.
- A monitoring note will be placed in the Agency file for next year to follow up.
- Strategies to End Homelessness will be notified of positive outcome via email.

Response 3

- A letter from PCL will be mailed to the ED of the Agency, copied to the project supervisor indicating the findings of the monitoring and informing them that the issue has been referred to STEH for action.
- Strategies to End Homelessness will be notified via email.

Messaging System Policy

Policy: The VESTA client messaging system was developed for the convenience of clients and Agencies and should not be used in any manner which compromises confidentiality or integrity of the system. The messaging system can supplement, but not replace, other methods of contacting homeless clients or other clients served by projects using VESTA.

Procedure:

- Only authorized Users at participating Agencies can enter messages. Only staff has direct access to messages. The system is designed to convey only minimal information, and requires a phone call back to the Agency that placed the message.
- Placing a message in the system is NOT adequate formal notice for legal, benefit, or health related issues.
- Agencies must determine and enforce their own message policies. It is up to the Agency to determine how and whether they will accept messages for clients directly, if they will post messages from providers outside the Agency, and if they will try to contact clients no longer receiving services.
- Government and service Agencies who are not HMIS participants may wish not use the messaging system to attempt to contact their homeless clients. In such cases, the organization should contact The Partnership Center for message placement.
- Messages that violate these terms will be removed; violators will be warned; repeat violators will be terminated as Users of the system.
- Since phone numbers and staff names are well known in the community, Agencies whose identity conveys protected information should not use the messaging system.
- Agencies should not place detailed information in the messaging system. For example, an Agency may notify a client to contact a lab regarding test results, but should not include test results in message.
- Users may not use the message system to store inappropriate information or communicate information about a client to other shelter workers. Doing so is a violation of User agreements, which specify that information in the system may not be used to deny housing. (Note: this means shelters cannot use the message for “bar out”.)

Outreach Exit Policy

Policy: All street outreach project clients that obtain housing should be exited from the street outreach project within 30 days of their housing start.

Procedure: This policy is designed to facilitate consistent data quality among street outreach projects using VESTA and to ensure an accurate picture of which projects' clients are active at any time. Review of VESTA data suggests that clients historically remained active in street outreach projects long after they obtained housing (and presumably are no longer working directly with outreach staff). The 30 day window is reflective of the fact that initial housing options are not always a suitable fit for clients, and sometimes it is necessary for the outreach staff to remain engaged with the client if they immediately fail out of that housing option, and return to the streets.

Likewise, this policy is not designed to encourage outreach projects to prematurely exit clients if their housing status is unknown (i.e. projects should not exit a client just because they have not seen them in a 30 day period). The policy applies only to exits for clients who are known to have obtained (and maintained) housing.

Street Outreach Homeless Certification Policy

Policy: To ensure consistent and accurate verification of homelessness before issuing a street outreach homeless certificate in VESTA.

Procedure:

- Street Outreach Homeless Certificates can only be issued for individuals sleeping outside, in camps, abandoned buildings, cars, or other places not meant for human habitation.
- Street Outreach Homeless Certificates cannot be issued to individuals who are staying in shelters, transitional housing, staying with family or friends, couch surfing, staying in hotels/motels, or are facing potential eviction from their own housing.
- When an individual requests a Street Outreach Homeless Certificate, outreach workers should ask specific questions to assess his/her current living situation. Questions could include, but should not be limited to:
    - "Where did you sleep last night?"
    - "Where will you sleep tonight?"
    - "Why do you need a Homeless Certification?"
- Individuals should be offered options of shelters where they could go to sleep.
- Individuals should be informed that outreach workers will verify the person's homeless status within one week, and that such verifications happen at various times during the Monday-Friday work week. Outreach workers should not provide the individual a specific day/time that outreach workers will be going out to verify their homeless situation.
- When verifying homelessness for an individual, outreach workers will look for evidence that the individual is staying at the location reported. Such evidence could include, but is not limited to:
    - Clothes
    - Bags of personal items
    - Empty food containers/bags
    - Shelter structure/tents/blankets/sleeping bags
- After verifying homelessness, outreach workers will enter client information into VESTA within 48 hours.
- Street Outreach Homeless Certificates are valid for 90 days. If an individual still needs a Homeless Certificate after 90 days, an outreach worker will need to re-verify their homeless status/living situation following the procedure outlined above and update the client's VESTA profile as appropriate.
- When deciding whether to issue Homeless Certificates, Outreach workers are to use their professional judgment and collaborate as needed with other professionals working with the homeless population.

System Usage Policy

Policy: In order to control for data quality, all participating Agencies must participate in required training and follow all established User protocols.

Procedure:

General HMIS Users:

- Only authorized Users may view or update client data.
- Agencies may have an unlimited number of Users of the HMIS system; each must have his or her own username and password, and these passwords are not to be shared.
- Each User must receive training from The Partnership Center in the use of the HMIS system.
- Agency directors (or designee) must approve each individual User from their Agency.
- Only paid staff (or approved students/interns) of participating Agencies may be Users of the HMIS system. Access permission is contingent on continued employment by the Agency, and will be terminated immediately if the User is no longer employed by the Agency. Each User must sign an agreement accepting system rules and protocols and receive training from PCL before receiving a username and password to access the system. These agreements must be renewed annually or User access to the system will be revoked.
- The Agency is responsible for supervision of Users and assuring that security, confidentiality, and data integrity are maintained.
- The Agency will report any breaches of confidentiality, consent, and actual or suspended misuse of data or the VESTA software system to PCL immediately
- PCL may terminate an individual's User access rights upon violation of confidentiality provisions. The User's supervisor will be notified immediately. Termination of an individual User will not necessarily affect the Agency's overall participation in the system. Reinstating the User will be determined through discussion with the Agency's Executive Director (or designee), STEH, and PCL.

Advanced Data Users:

- Because of the complexity of the database, specific training on Flexo (VESTA's custom report builder tool) will be required prior to its use.
- Agency Directors (or designee) must authorize a User to be trained in Flexo.
- Any deliberate misuse or misrepresentation of VESTA data by an Advanced Data User may be considered cause for termination of the User's agreement.

Unduplication Approach

Policy: An HMIS must be capable of unduplicating client records with distinct Personal Identification Numbers automatically matching personal identifier fields (e.g., name, SSN, date of birth, and gender). This functionality must be able to unduplicate counts of clients and to support accurate HMIS reporting. This requirement applies to all client records entered in the HMIS, including client records entered by CHOs that have not been disclosed to other CHOs (non-consenting client records). VESTA System Administrators are allowed to edit a client record in order to facilitate unduplication. This includes correcting a client's recorded gender, correcting misspelled names, or entering a SSN into a record which doesn't have one.

Procedure:

1. Each **client ID** is a link to a client's record. If basic client information is edited, VESTA saves those changes.
2. When one client record is **missing information,** (field left blank, field 'unknown', or field selected as 'client doesn't know', 'client refused', or 'data not collected') but the other client record contains the missing information, merging the records will automatically discard unknown data and use available data.
3. When one client record is YES for **Consent** but the other record is NO for Consent, regardless of the 'Select Target', after merging the final client record will be marked as consenting.
4. If two records exist that can be merged, where possible, the smaller (i.e. older) **Client ID** number will be the target record. The smaller the Client ID number, the earlier that client was created in VESTA.
5. When one client record contains a selected **race** and the other client record contains a different race, when the records are merged the client will show as having both (multiple) races.
6. In certain cases, other discrepancies can be resolved directly by VESTA system administrators. These cases are described below:

Client name discrepancies:

- One client record contains middle name or middle initial but the other record is missing middle name.
- One client record contains middle initial but the other record contains the full middle name (both beginning with the same letter).
- One client record contains 'Other Names' but the other record does not contain 'Other Names'
- The names in both client records are different only due to case sensitivity.
    - **Action**: Merge with the target being the client with more data in the name field, e.g. the client who has the full middle name. If necessary, edit the target client record so it contains the full/correct middle name and has correct capitalization of all name elements.

Gender discrepancies:

- One client record contains one gender but the other client record contains another gender AND…
    - the name is very clearly gender-specific.
    - or a client photo shows the client to be obviously male or female.
    - or the client is present in a project which only serves a particular gender (e.g. a family shelter doesn't serve adult males).

      Action: Change the gender in the record that is incorrect.
- If one selected gender is transgender or the gender of the client is in any way ambiguous, an email must be sent to confirm the gender to the Users who entered the most recent intake on each client (see #7 below).

SSN discrepancies:

- One client record contains a complete SSN but the other record contains a missing SSN (000000000) AND all of the remaining information is identical.
    - **Action**: Merge the two records with the target being the record with the full SSN.
- One client record contains a partial SSN (e.g. "000007742") and the other contains the full SSN (ending in …7742). Remaining information matches.
    - **Action**: Edit the source record with the partial SSN and give it the full SSN of the target record.

7. An email must be sent to both VESTA Users who did the most recent intakes if any other ambiguities exist for the merging of two client records. Cases where this procedure is necessary include:
    - The client records contain different names (this does not include situations where the only difference in the names is case sensitivity, OR where the first and last names are the same and the only difference is a missing middle name, middle initial, or other name/nickname).
    - The client records contain different genders and other information provided for that client does not clearly distinguish with certainty the gender of the client.
    - The client records contain two different SSNs (where neither is an invalid SSN 000000000 NOR where one record contains a partial SSN ending or beginning with matching numbers in the full SSN--e.g. SSN 123456789 and SSN 000000789).
    - The client records contain different DOB.

8. If an email is sent to both Users who did the most recent intakes on the client records in question and no reply is received from either User or the Users cannot recall the information that needs to be confirmed, then the records cannot be merged at that time.

User Access Levels

Policy: In order to properly regulate access to data and reporting amongst various Users within the database, VESTA had established User access levels that govern whether Users can view/add/edit project data and/or generate reports on the data.

Procedure:

- All VESTA Users are assigned a User access level for each project to which they are granted access, as determined by their Executive Director (or designee). A User who has access to multiple projects within an Agency may have the same or different access levels for each project.
- Changes to project access levels can only be requested by a User's Executive Director (or designee)
- The following is a list of the primary User access level for VESTA Users (Note: there are some additional access levels that are used only by STEH or PCL Staff to facilitate administrative or User Support functions):

  Regular: Client data entry/editing and review- no access to reports
  Power: Full access to client data entry/editing, review, and reporting
  Supervisor: Full access plus view all Users' error alerts for project(s) with Supervisor access
  VESTAcard: Access only to VESTAcard module; no full VESTA access
  Reports only: View and print reports only- no access to individual client records
  Data updater: Very limited client data entry- requires special arrangements

Training Policies and Proceedures

Training Policies and Proceedures

Training Curriculum

Policy: All new Users are required to complete at least one training session prior to having access to VESTA. The training requirements are as follows:

VESTA 101

VESTA 101 is a training designed to ensure that each new User learns the basic skills to navigate VESTA, including recording client details and services, and any other aspect of VESTA use necessary to performing his/her job.
This training is required for all new HMIS VESTA Users and new EA employee VESTA Users.

Scheduling: After a User Set-Up form has been received and processed by PCL, the User Support Team will contact the User's supervisor(as listed on the form) to schedule the VESTA 101 training. Typically, the training will be scheduled at least one week after processing the Set-up request.
Time Length: One (1) hour for regular, power, and supervisory Users; 30 minutes for VESTAcard and reports only Users.
Format: On-site training at User's work location (one-on-one or small group)

EA in VESTA: From Food to Stability

EA in VESTA: From Food to Stability is a training tailored to all new volunteers and student interns at emergency assistance programs. The training provides a general background of VESTA, basic skills necessary to navigate VESTA (such as those covered in VESTA 101), and EA specific skills. **This training is required for all volunteer, student, or other non-staff, and can also be provided by an Agency VESTA-authorized trainer.**

Scheduling: Users can schedule their attendance on PCL's website using the registration page. Trainings are held once or twice monthly depending on demand.
Time Length: One (1) hour
Format: Training conducted in PCL's training facility, 2134 Alpine Place, Cincinnati, Ohio 45206

Procedure:

- These initial training classes are designed to allow the User to navigate the system with User Support

supervision rather than the trainer leading the session.

- At the conclusion of the training session, the User is asked to sign a training outline indicating that they have been trained on and understand how to utilize the VESTA software. In addition, each User must sign a User agreement outlining the policies and procedures governing access to the system and security of the data. This agreement is re-signed at least annually or whenever a User seeks access to a new project.

Supplemental Training/Timetable

Policy: Beginning in 2016, all new Users will be required to complete a follow-up group class within 90 days of completing VESTA 101. HMIS Users who hold part-time/ overnight/ or weekend only positions may receive an exemption from this class. In addition, PCL regularly offers additional training opportunities for VESTA Users. The training requirements are as follows:

The Power of Together®

The Power of Together® training is a fun and interactive training designed to provide Users with a better understanding of VESTA as a community level database, with a strong focus on the homelessness continuum. This training provides new Users the opportunity to network with each other, all while mastering the basic skills needed to successfully use VESTA for their jobs. **This training is required for all new VESTA Users who are new to the Agency, and/or new to homelessness or emergency assistance services (within 90 days of completing VESTA 101) and is recommended for longer-term emergency assistance volunteer Users.**

Scheduling: Users can schedule their attendance on PCL's website using the registration page.
Time Length: One (1) hour
Format: Training conducted in PCL's training facility, 2134 Alpine Place, Cincinnati, Ohio 45206

Procedure:

- The Power of Together is offered monthly, on a first come, first serve basis.

VESTA+ hours

The VESTA system is constantly changing and improving. In order to ensure that long-standing VESTA Users are familiar with the newest features, VESTA Users are asked to complete additional trainings, VESTA+ (plus) hours, every year. These training hours are similar to continuing education hours required for social work credentials, but are specifically geared towards VESTA. VESTA+ hours are required on an annual basis after Users' first year of VESTA use. All regular, power, and supervisory Users must complete at least 4 hours of VESTA+ hours per year (VESTA Card only and Reports only Users must complete at least 2 hours per year) to maintain their level of use. VESTA+ classes will be revised periodically and class topics will be published on the PCL website's registration page as they are developed.

Procedure:

- PCL will maintain a training calendar with supplemental training opportunities at least monthly for small groups of Users to learn more about specific VESTA topics.
- In instances where significant changes are made to VESTA, The Partnership Center Limited (PCL) routinely offers group sessions to provide instruction of new features/ functionality.
- For advanced Users interested in building their own custom reports, PCL periodically offers the Advanced Data Users Academy. This course trains Users in the use of Flexo, a custom reporting tool that allows Users to generate and save ad-hoc reports to provide customized information for funders, boards, etc.

EA Train the Trainer

Policy: For Emergency Assistance Agencies with a dedicated volunteer coordinator or staff who directly manage volunteers, the EA Train the Trainer curriculum prepares and certifies Agency staff as a VESTA trainer for new

volunteer (un-paid) Users.

Procedure:

- Generally, EA Agencies may only certify one paid staff as the VESTA trainer for volunteer Users at the Agency.
- In order to become certified, staff must participate in an initial training and successfully complete a mock training exercise; and complete a yearly renewal course.
- Certified Agency trainers must demonstrate their use of PCL provided training materials and must adhere to the training outline, covering all necessary topics with each new User.
- Certified trainers may be asked to participate in additional trainings if monitoring by PCL (including data quality of volunteer Users, set-up requests, and the trainer's data quality/ User performance) indicate additional need. If User performance does not increase or PCL has information that the trainer is not following appropriate training protocol and/or the new User set-up process, PCL may revoke the staff's certificate as a trainer.

VESTA Medicaid Application Project Training

Policy: For Agencies with paid staff Users who provide benefits assistance to clients, the VESTA Medicaid Application Project training prepares Users to submit benefit applications through the Medicaid Application Project within VESTA. This does not apply to Agencies with a current relationship or special process for benefit applications – such as a dedicated Hamilton County Jobs and Family Services worker.

Procedure:

- A User must participate in a Medicaid training prior to accessing the Medicaid Application Project within VESTA.
- In order to participate in the training, Users must meet the following pre-requisites:
  - User must hold a paid staff position within the Agency;
  - Demonstrate work experience or current work duties related to assessing individuals for benefits, directly assisting in benefit acquisition, financial coaching, or benefit advocacy;
  - Maintain appropriate VESTA User performance and demonstrate a high familiarity with VESTA.
    - VESTA User performance will be determined by PCL Staff and will look at the following:
      - Previous VESTA experience
      - Number of Error Alerts – Are they within acceptable limits? Is the User under any active error monitoring?
      - Data Quality – Is the data quality for items related to the Medicaid Application Project (such as social security number, income, non-cash benefits, health insurance/medical benefits) generally no more than 2% of clients with missing data?
- Once trained, Users will be required to annually sign a User agreement specific to the Medicaid Application Project.
- During the first year of this project, PCL Staff will continue to monitor trained Users, and User access will generally be limited to two Medicaid application Users per Agency.
- If at any time Users fail to maintain appropriate VESTA User performance, PCL Staff may require additional training or turn off User access to the Medicaid Application Project.

Roles

Policy: The VESTA User Support Team is responsible to train and support the Users of VESTA.

Procedure:

- Technical and User Support questions are generated through email and phone calls from Users and are addressed in a timely and accurate manner.
- User Support Staff regularly interacts with the VESTA development team so they can be kept abreast

regarding User interface issues, bugs or other items that affect the User's system experience and improve service delivery to our customers.

- User Support Staff also assists in the development process for training and implementation of new features. This includes testing of new/modified reports, projects, and other system enhancements prior to deployment.
- User Support Staff has a limited scope to only assist with technical issues directly related to VESTA functionality (for example assisting with browser settings and digital certificates) and troubleshooting equipment if it was provided by PCL (such as signature pads).

Security Policies and Procedures

Security Policies and Procedures

Tuberculosis (TB) Policy

Policy: Tuberculosis is a serious health threat to the homeless and the community at large. Every effort should be made to cooperate with local health officials to minimize contagion.

The data in VESTA is owned by the Agencies and is subject to local consent procedures. It is the responsibility of each Agency, when approached by local TB Control officials, following the official opening of a TB Contact Investigation, to release their specific Agency data to TB Control.

Procedure:

1. To facilitate release of TB Control related data, a report in VESTA lists the name, date of birth, and number of days an individual has been sheltered during the given date range. Agencies should, at the request of TB Control, run that list and provide a printed hard copy or an Excel spreadsheet of the data to TB Control. It is the obligation of the local Agency to work with TB Control around the release of their data.

2. PCL programming staff can query the data in simple or sophisticated ways to assist an Agency in a search during a Contact Investigation. TB Control may request additional information of a homeless provider Agency and the Agency may choose one of two methods to request specialized data queries of PCL:
   a. An Agency may determine with TB Control what queries will be authorized and make the request directly to PCL. PCL Staff will work with the Agency and data will be provided directly to Agency, the Agency may release the information to TB Control, subject to the Agency's policies and procedures.
   b. The Agency may authorize PCL to work directly with TB Control. In this case, PCL will require a written authorization from the Agency director (via email or post) prior to working with TB Control. In this case, PCL will provide data directly to TB Control with copies to the Agency director.

3. Confidentiality standards imposed by local VESTA Advisory Board for VESTA do not permit any Agency to see <u>all</u> the residential and/or service projects a homeless person has utilized during a period of time. Only a PCL VESTA System Administrator can view this information. **Pursuant to the HMIS Data Standards "Protected Personal Information maintained in HMIS (like other data systems) also *<u>may</u>* be released for the following reasons: 1) if required by law; 2) to avert a serious threat to health or safety…"** Accordingly, when TB Control has initiated a formal TB Contact Investigation, they may formally request PCL to review the individual's data associated with the Investigation and to release to TB Control the history of any known associations and contacts within these locations. PCL will work directly with TB Control, once proper authorization has been provided, to identify all locations the client had contact with during the Investigation Period. TB Control must provide the full name, SSN, and/or Date of Birth of the homeless

individual with TB, if they have it, along with any other identifying information that will enable PCL to identify the individual in the database. Pursuant to HIV confidentiality standards, specifically OAC3701-3-03 (c), HIV information may only be released to the Health Department upon their direct request.

4. Upon identification of an infected individual's history of shelter stays and/or contacts within VESTA, PCL will work with TB Control to notify case workers and other homeless individuals (clients) who were exposed to TB via contact with the individual as follows:
   a. Client notification will be done using VESTA. Each client exposed to TB will have an icon next to his/her name on Active Client Lists/Client Summaries; this icon will be visible at any project the client is served. Clicking the icon will display a message about TB exposure and referral information.
   b. Users who deliver this message to clients will mark the message as 'delivered' so that PCL will be able to analyze the effectiveness of this system.

User Security Components

Policy: The User security components help VESTA keep client information confidential and efficiently respond to Users that are misusing the system.

Procedure:

- Only authorized Users may view or update client data
- Agencies may have an unlimited number of VESTA Users, each must have his/her own username and password
- Each User must receive training in the use of VESTA
- Agency directors (or designee) must approve each individual User from their Agency.
- Only paid staff (or authorized students/interns) of Agencies may be Users of the VESTA system
- Access permission is contingent on continued employment at the Agency, and will be terminated immediately if the User is no longer employed by the Agency. It is the responsibility of the Agency to notify PCL prior to or upon the termination of the employee. PCL will terminate access immediately.
- Each User must sign a User agreement stating full understanding of the system rules and protocols before receiving a username and password to access the system. These agreements must be renewed annually or User access to the system will be revoked.

Student/Intern Access Policy

Policy: In general, only paid Agency staff is granted access to HMIS projects in VESTA. However, under certain circumstances, Agencies may request access to VESTA projects for students and/or interns.

Procedure:

Access for such Users will be considered under the following conditions:

- Access to VESTA will only be allowed from the student/intern's primary physical work location. This restriction will be enforced through the use of a digital certificate, IP address tracking, or other measures deemed appropriate by PCL.
- Executive Directors (or designees) must provide assurance, in writing, that the student/intern's VESTA use will be actively monitored by a paid staff person(s) to ensure that only data necessary for completion of their assigned duties is being accessed, and, if applicable, all data entry is being performed properly.
- Unless strictly required by their assigned duties, student/intern access should not include viewing/editing of client-level data.

Just like any other User, prospective student/intern Users will receive the appropriate training formal VESTA training by PCL Staff or a certified Agency VESTA trainer before obtaining access to the system. Given the frequency and turnover of student/intern assignments, it is not practical for PCL to provide one-one on-site

training for every student/intern User. Instead, PCL offers group training, as often as monthly if required, for students/interns requiring access. This training will be provided free of charge provided trainees attend (unexcused absences without 24 hours' notice will incur a fee). As with any other User, it is the Agency's responsibility to notify PCL immediately when a student/intern's assignment is complete and their access to VESTA can be terminated.

VESTA User E-mail Policy

Policy: Primary communication between PCL and VESTA Users is conducted via e-mail. In order to ensure that information disseminated to Users does not result in unauthorized access or compromised confidentiality, specific requirements for User e-mail addresses have been established.

Procedure:

1) Every VESTA User must have a unique e-mail address, which must be provided to PCL User Support upon initial VESTA User setup. VESTA Users may not share an email account.
2) For security reasons, e-mail addresses used for VESTA communications must utilize the Agency's e-mail domain (for example, username@ABCagency.org) or may be a generic web-based e-mail account as long as the email was created by the Agency for the employee's business-only uses. In the event that a given Agency does not have a designated e-mail domain, PCL User Support will work with that Agency to establish an alternate e-mail protocol that will maximize the security of VESTA-related communications via e-mail. Under no circumstances will VESTA e-mail communications be directed to User's personal e-mail account.
3) In the event that a User is employed separately by more than one Agency, that User must have a separate VESTA username for each Agency, and each username must be associated with a discrete e-mail address meeting the requirements listed above. (Note: separate accounts/e-mail addresses will not be required in cases where a User employed by a single Agency is accessing multiple Agencies' projects based on the existence of a partnership agreement allowing shared access between these Agency projects.) If a User is authorized to have VESTA access by multiple Agencies, it is PCL's policy to notify the Executive Director of each Agency to verify that they are aware of such multiple Agency access.
4) User set-up agreements submitted to PCL User Support without an e-mail address or with an address that does not adhere to this policy will not be processed. Users will not be granted access to VESTA until an appropriate e-mail address has been verified. Please note that this policy pertains to both paid Agency staff and student/intern Users (if applicable).

User ID/Password/Personal ID Number Specifications

Policy: Access to any HMIS application must be secured with a User authentication protocol, a methodology for ensuing that only authorized Users are permitted access. The confidentiality, integrity, and availability of an HMIS application are dependent on preventing unauthorized persons from accessing or altering HMIS data.

Procedure: VESTA utilizes a multi-tiered approach to User access security:

1) Each User is assigned a unique username. In most cases, it consists of the User's first initial and last name.
2) At their initial VESTA login, each User is required to designate a unique password known only to them. A password must have at least eight non-blank characters, contain at least one letter and one number, and may not be the same as the User's username. Passwords are required to be reset every 90 days.
3) As part of an effort to streamline access to VESTA for Users while maintaining a high level of security for data, VESTA has an additional security method based on Internet Protocol (IP) address filtering and a PIN code requirement. Under the IP address filtering system, VESTA tracks the unique internet location from where a given User is accessing VESTA. As a general rule, the IP address (a string of 12 numeric digits) for a specific facility or location tends to stay the same over long periods of time. However, no two internet gateways can have the same IP address at any given time. Thus, if the same User accesses VESTA from their office and then later that day from another location, VESTA records the access from two different locations and of course whether or not the login was successful.

In order to ensure that an authorized User is attempting to access VESTA from a new location, every VESTA User is required to establish a personal 4 digit PIN. Once the PIN is established from their primary work location, the User is only asked to enter it when accessing VESTA from an IP address they have not accessed from before, or in the unlikely event that their work location IP address changes. This feature is designed to safeguard against a situation where a User's username and password have been compromised. Since it is highly unlikely that someone attempting to gain unauthorized access to VESTA would do so from the authorized User's work location, without the PIN, a hacker would not be able to log in from a remote location. The PIN is also required when a User wishes to reset his/her password. Furthermore, after four attempts with the incorrect PIN, the User's account is locked and can only be unlocked by a VESTA system administrator.

4) A final security feature is the selection of three security questions/answers provided privately to VESTA User Support by each User. Similar to technology implemented by banks and other secure online sites, PCL developed a list of personal questions (from which the User choose three) where the User is likely to be the only person who knows the answer. Once provided, these questions are then locked away in the User's profile where they can only be accessed by VESTA system administrators or the Users themselves after successfully logging in. These security questions and answers serve to positively identify a User to User Support Staff if there is any ambiguity as to who is calling on the phone. In the event that a User is either a) locked out of VESTA for too many incorrect login attempts or b) attempts to access VESTA from a new location and doesn't recall their PIN, the User can call VESTA User Support, provide the answers to their security questions, and have their password reset or account unlocked.

VESTA Dormant User Policy

Policy:

In order to maximize VESTA security, only Users who are accessing VESTA on a routine basis (or who are accessing limited features at specific intervals) should have active User accounts. A current VESTA User Agreement by itself does not signify an "active" User. User accounts are monitored to ensure that Users with valid accounts are using the system on a regular basis.

Procedure:

PCL will review User activity across the entire VESTA system at regular intervals. Dormant User accounts (those who have not accessed the system for at least 6 months) will be handled as follows:

- A User who has not accessed VESTA login for 12 months or longer will be deactivated. This policy will be implemented regardless of the status of the User's VESTA agreement. Such accounts will only be re-activated at the specific request of the User's executive director. Any User who has not used VESTA for more than 12 months MUST be re-trained in order to have their access restored.
- For Users that have not accessed VESTA in between 6 months and 1 year, VESTA User Support Staff will generate an e-mail notification to the User and key contact/supervisor requesting a determination of whether access is still needed for that User. This notification will specify that a request for continued access be received from the key contact/supervisor within 5 business days or the User's account will be deactivated. Such accounts can be re-activated at a future date upon request of the Agency director. Re-training of such Users will be offered on a case by case basis.

Remote Desktop Viewing and Control

Policy:

Partnership Center, Ltd. User Support Staff can provide remote support only on-demand software that encrypts the network traffic (VESTA remote) or through utilizing "go to meeting" screen sharing tool. Remote sessions may only be initiated by direct action of the VESTA end User requesting assistance.

Benefits:

1. Faster service: Partnership Center, Ltd. support staff can provide immediate support to Users by viewing exactly what the User is viewing in their VESTA session.
2. More responsive service: User Support Staff can quickly diagnose and resolve the issue and, if necessary, elevate issues to the attention of appropriate VESTA personnel for troubleshooting.

Procedure:

1. VESTA remote
    a. Access may ONLY occur with the expressed written authorization of this policy by the Agency director. PCL will not remotely access any User's computer (nor initiate the installation of any software that would enable this functionality) unless such an approval is on file for that User's Agency.
    b. Users must initiate the remote session by downloading and installing the approved application. In most cases, these sessions will not require administrative or other enhanced access to install.
    c. Users must communicate a session-specific, randomly-generated access key in order for PCL Staff to open the connection.
    d. All remote access communication will be encoded and encrypted using recognized industry standards. In most cases, remote access will not require modification to firewalls.
    e. Remote sessions allow for view screen only access or full remote control at the request of the User.
    f. Users can terminate the remote session at any time, and in the event of remote control, the User's commands always take precedence over remote commands initiated by PCL Staff.
2. Go to Meeting
    a. Screen sharing must be initiated by the User.
    b. PCL Staff will provide a link to begin the meeting and the User must click to share his or her screen. Using this tool, PCL will only be able to view the screen to guide the User to resolve the question.
    c. Users can choose to stop screen sharing or end the meeting at any point.

Incident Response Plan

Policy:

To protect the data in VESTA and the integrity of VESTA as a community level database, procedures have been put in place to ensure consistent responses to incidents (such as security breaches and/or inappropriate User, project, or Agency actions). This plan is intended to address how PCL will respond to any incident, including: assessing the incident, minimizing damage, ensuring quick response, and documenting and preserving evidence.

Incident Definition: An incident is any one or more of the following:

- Loss of information confidentiality
- Compromise of information integrity
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Misuse of information, tools, etc.
- Sharing login information
- Infection of systems by unauthorized or hostile software
- An attempt at unauthorized access
- Unauthorized changes to organizational hardware, software, or configuration
- Reports of unusual system behavior

Procedure: PCL will use the following guidelines when addressing any incident in relation to VESTA.

1. **Discovery**: Typically an incident will come to the attention of PCL when someone discovers something not right or suspicious. It may be discovered by:
    - User Support
    - Intrusion detection system
    - A system administrator
    - A firewall administrator
    - A business partner
    - A monitoring team
    - A manager
    - Agency IT staff
    - An outside source
2. **Assess and document the issue**; including but not limited to:
    - Scope of the issue – how many clients were affected? How many Users involved?
    - Whether the situation resulted from a User acting on his/her own, under the direction of a supervisor, and/or due to a general culture of the project or Agency.
    - Is the incident still in progress?
    - What data or property is threatened and how critical is it?
    - What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    - What system or systems are targeted, where are they located physically and on the network?
    - Is the incident inside the trusted network?
3. **Determine the response and minimize damage**: In order to minimize risk and respond quickly, PCL may act initially on its own to determine the appropriate response strategy. In determining the strategy; the following questions will be considered and an incident level will be assigned.
    i. Considering questions:
        - Is the response urgent? (Scope and nature of the incident?)
        - Can the incident be quickly contained?
        - Will the response appropriately alert those involved in the incident?

    ii. Incident Level System (ranked from most severe to least)
        - Category 1 - A threat to the community-wide security of VESTA
        - Category 2 - A threat to shared data elements in VESTA
        - Category 3 - A threat to VESTA security within an Agency or across shared projects
        - Category 4 - A threat limited to the scope of actions of one User

    iii. Responses: Based on specific situations that have arisen in the past, the following guidelines have been established to help guide PCL's initial response. *Please note: New situations are likely going to arise that may require additional responses.*
        a. Isolate and contain the incident
            i. Category 1 and 2 – This may result in temporarily turning off a particular feature, field option, or sharing agreement.
            ii. Category 3 and 4 – This may result in temporarily turning off an Agency, project, or specific User.
        b. Notify appropriate parties and begin to address the issue:
            i. Notify - All the following parties will be notified immediately if any action is taken:
                1. Agency: Executive director, direct project management, and specific Users involved
                2. Funders: In the case that the Agency/ project is using VESTA as a requirement of their funding, the primary contact for the funder will be notified immediately
                3. VESTA Advisory Board: Advisory chair and committee will be made aware of the incident and response.
        c. Addressing the issue - PCL will work quickly with the Agency, funder(s), and VESTA Advisory Board, as appropriate, to quickly resolve the issue. If necessary, PCL will convene all the parties together as quickly as possible to discuss an appropriate action plan to resolve the incident. This is intended to ensure all viewpoints are addressed and considered as part of the action

plan. If necessary, the VESTA Advisory Board may convene prior to its involvement to ensure that the Board agrees with the viewpoint it is taking on the incident.

i. Establish Action plan - Based on incidents arising in the past, an action plan may include:
    1. Agency leadership and PCL addressing the actions of staff and determining if additional action against the User is appropriate
    2. Agency leadership establishing or modifying Agency policies around VESTA usage and ensuring staff are properly notified
ii. Restore Access – In cases were an action plan is initiated, PCL will restore access once the action plan is established and any immediate steps are taken.
iii. Monitoring Action Plan – As part of the action plan, PCL will work to ensure that a monitoring plan, if necessary, is included as part of the action plan.

d. Terminate specific Users' access
    i. In severe cases, PCL will adhere to a zero tolerance approach. Without prior warning to the User, PCL may choose to ban the User from future access to VESTA (i.e. - cases where a trained User has knowingly and intentionally shared his/her personal password and login).
    ii. In other cases, PCL will notify the User and supervisor of the issue as a warning, but if the User commits the same or similar action again, PCL may ban the User from future access, temporarily suspend the Users' account, and/or require the User to complete additional training before turning the User's access back on.
e. Final Resolution: In the case that the Agency, PCL, and/ or funder are unable to come to an agreement of action to resolve the incident, PCL maintains the right to terminate system usage for any Agency that violates or compromises client confidentiality based on access to or use of the system. Any Agency wishing to contest the termination may seek mediation from the Cincinnati Mediation Association, and will be responsible for all charges and/or fees incurred from the mediation.

4. **Document the incident**: All documentation of the incident and response will be stored in PCL corporate files. Any documentation referencing client files will either use the Public ID or the Client ID as the key reference code to the file stored in VESTA.
5. **Notification:** Notification of incidents is important as VESTA is a shared, community-level database, and the HMIS in Hamilton County. Beyond the notification step as part of any response, there may be necessary times to notify other groups, such as: EA leadership, Clearinghouse, and general Users. When necessary, PCL may post a general warning or notice to all Users on VESTA to alert them of the incident and response or provide a more detailed account of the incident, response, and resolution.
6. **Assess damages and costs**: If necessary, PCL will assess the damages to VESTA and/or the costs associated with responding and fixing the incident.
7. **Review response and update policies:** After any incident PCL will plan and take preventative steps so that the possibility of the incident occurring again will be minimized and update these policies as needed. The following will be considered:
    - Whether an additional policy could have prevented the intrusion.
    - Whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
    - Was the incident response appropriate? How could it be improved?
    - Was every appropriate party informed in a timely manner?
    - Is additional monitoring necessary?
    - Were the response procedures detailed and cover the entire situation? Can they be improved?
    - Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    - Have changes been made to prevent a new and similar infection?

- Should any security policies be updated?

8. **Incident Preparation and Prevention.**
   i. **Preparation:** PCL currently has the following in place to limit incidents from occurring initially: (Please note that this list is not exhaustive.)
      - Security training with all new Users
      - Signed agreements outlining liability as a result of misuse of VESTA (User agreements, Agency agreements, sharing/ partnership agreements)
      - Security such as individual passwords that require change on a regular basis, tracking of IP addresses, Digicerts for volunteers, Notices to TechSupport when a User attempts to access VESTA outside of his/her privileges, User level set-ups, etc.
      - Secured servers
      - Automatic log-off after inactivity
      - Dormant User policy
      - Designation of a VESTA contact per Agency to ensure communication from VESTA is distributed to the Agency as needed
      - Error alerts
      - Monitoring reports and processes

   ii. **Prevention of re-infection.** After any incident, PCL will take steps to prevent an immediate re-infection which may include one or more of:
      - Close a port on a firewall
      - Patch the affected system
      - Shut down the infected system until it can be re-installed
      - Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
      - Change email settings to prevent an attachment type from being allow through the email system.
      - Plan for some User training.
      - Disable unused services on the affected system.

Central Server Operation, Maintenance and Data Security Plans/Commitments

Central Server Operation, Maintenance and Data Security Plans/Commitments

Server Access (via networks)

Policy: HMIS vendors, HMIS Leads, and CHOs must ensure that computers, devices, and servers on which HMIS applications and data are stored or processed are protected from malicious intrusion behind a boundary protection device ("firewall") that is configured to allow only ports and services that are required in the course of regular operations.

Procedure:

1. The VESTA servers are protected behind an intelligent firewall device which blocks traffic incoming to the VESTA servers except for:
   - HTTP
   - HTTPS ("SSL")
   - Private encrypted VPN (virtual private network) traffic between the servers and authorized

Partnership Center computers.

2. Additionally, the VESTA servers also make use of the built-in Windows firewall software to further restrict incoming traffic to the computers.
3. By default, Windows-based servers and workstations have their software firewall enabled and it is general expected that it remains so for all workstations accessing the VESTA website. Naturally, standard firewall exceptions are expected such as those which permit file sharing or remote administration of systems.

Server Access (physical location)

Policy: Physical access to servers which store HMIS data is limited to authorized HMIS system administrators from PCL.

Procedure:

- VESTA-Live equipment resides at the Cincinnati Bell/CyrusOne downtown Cincinnati Data Center.
- Only select PCL Staff has direct access to the VESTA server rack. Anyone requesting access to it must be positively identified as an authorized person before even gaining access to the building. Additionally, a data center employee must unlock the cage to allow access to the servers.

Audit Trails

Policy: HMIS software must track User activity in the HMIS.

Procedure:

VESTA logs the following events and retains a rolling one-year history in the active VESTA-Live database, with prior years being available in backups:

General events that apply to all VESTA Users**:**

1. Successful login.
2. Logout.
3. Unsuccessful login (username and password are not saved in audit log, though if supplied username matches an existing VESTA account the user ID is stored).
4. User requesting a password reset (logging occurs via email to VESTA User Support).
5. User automatically logged out of VESTA.
6. User redirected to the login page due to the same username being used in a successful VESTA login in another web browser window or on a different computer.
7. User accessing any page in VESTA, along with the URL of the page requested. This includes pages such as the VESTA home page, a client review page (including the client ID), intake or exit wizard pages, etc.
8. User being blocked from accessing a webpage in VESTA, along with the URL of the page requested.
9. User executing a report, along with all the parameters selected for report execution.
10. User experiencing an unexpected error (“YSD”) message, (details of error are emailed to VESTA Support).
11. The IP addresses from which a User accesses VESTA. Previously-unknown IP addresses require the User to supply their VESTA PIN before successful login.
12. When any client data is changed, VESTA maintains a history of “what was data before it was changed”.

Additional events logged for system administration functions**:**

1. Which administrator last edited a User account and when.
2. User accounts deactivated due to expired User agreements.

Backup and Recovery Procedures

Policy: In order to ensure that data entered into VESTA is safe in the event of a catastrophic power/system failure, a series of redundancy/backup/recovery protocols have been established.

Procedure:
VESTA-Live backup procedures have been optimized for speed in recovering data quickly while maintaining a reasonable history of "back in time" data snapshots.

1. All VESTA-Live servers use RAID-5 hard drive configurations for redundant hard drive storage.
2. The VESTA-Live transactional database is backed up nightly to another folder on the same server. There is a 30-day history of these nightly backups.
3. The VESTA-Live transactional database's transaction log is backed up hourly to another folder on the same server. There is at least a one-day history of these transaction logs.
4. The nightly and weekly backups of the VESTA-Live transactional database are mirrored nightly to another VESTA server in the same facility as the VESTA-Live transactional database server. Specifically, the VESTA-Live reporting database server.
5. The VESTA-Live transactional database is also backed up weekly to another folder on the same server, independent of the nightly backup. These weekly backups are maintained indefinitely.
6. The VESTA-Live transactional database is also backed up nightly to Cyrus One's off-site backup facility using Tivoli backup software installed on that server. These backups are available using the same Tivoli software on the server, or by requesting a copy through Cyrus One's online service ticket system.
7. The VESTA-Live web server copies scanned/uploaded client-related documents, including client photos, to the VESTA-Live reports database server.
8. The VESTA-Live web server performs a full Windows Backup of all its data on a nightly basis and stores this on the VESTA-Live reports database server.
9. The VESTA-Live reports database server also contains a mirror of all the database backups, both nightly and weekly, made on the VESTA-Live transactional database server. This mirror is updated nightly.

Internet Connection and Power Redundancy

Policy: As web-based software, VESTA relies on power and a working internet connection to ensure uninterrupted access for Users. Both must be redundant.

Procedure:

1. The VESTA-Live servers reside at the Cincinnati Bell/CyrusOne downtown datacenter. This datacenter has redundant incoming internet connections as well as generator-based power backup.
2. VESTA-Live servers require a minimum of 4 hours to relocate to a different facility in the event of a longer-duration power or internet outage at the Cyrus One datacenter. The VESTA servers can reside on a temporary basis at a facility with a single static IP address and incoming internet connection at least 3mbps.

Transmission/Encryption

Policy: The HMIS Lead, CHOs, and HMIS vendors must encrypt all HMIS data containing client protected personal information (PPI) that are electronically transmitted over the Internet, publicly accessible networks or phone lines in accordance with current industry standards using AES-128-bit equivalent or higher encryption. The HMIS application must implement these transmission standards for any transactions it processes.

Procedures:

1. VESTA uses the Secure Sockets Layer (SSL) protocol with 128-bit encryption. This provides a highly secure, encrypted connection between the VESTA server and the User's computer. SSL is an industry standard and is used on all websites where sensitive information is transmitted.
2. VESTA Users should not store files with PPI unsecured on their workstations.
3. VESTA Users should **never** email unencrypted PPI, and should be very careful about to whom PPI is sent.
4. When accessing, storing, or sending PPI, Users should consider "is this how I would treat data about myself?"

Virus Protection

Policy: The HMIS Lead and CHOs must protect HMIS systems from applications designed to damage or disrupt the system (e.g., a virus) by using anti-virus software. The HMIS Lead Agency and CHOs must update virus definitions from the anti-virus software vendor at least weekly.

Procedures:

1. All VESTA servers use Symantec Endpoint Protection, an industry-standard antivirus software, which updates automatically on an as-needed basis.
2. All workstations and servers which store VESTA code are also protected with antivirus software.
3. All workstations used to access the VESTA website must also have antivirus software set to automatically update at least on a weekly basis.

Technical Specifications

Technical Specifications

Hardware, Software and Connectivity Requirements

Policy: Agencies are responsible for purchasing and maintaining approved computer systems, operating software, networks, and internet access. Because of the confidential nature of data stored in VESTA and its use as a community database application, PCL requires that the system must be accessed from a secured and semi-private location. Computers located in public areas will not be granted access to VESTA. Each User must have their own unique username and password to access the computer/network from which they access VESTA. All computers that access VESTA must have up-to-date anti-virus software installed and running.

PCL will maintain the hardware and software required to support the VESTA system for community wide use; perform regular data backups of all data stored in VESTA; and complies with industry standards for security.

Procedure:

Minimum system requirements for User systems to access VESTA:

Hardware:	1.5 GHz processor
	512 MB RAM
	1 GB free hard drive space
	VGA (1024 x 768) display
Software:	Windows XP
	Microsoft Internet Explorer 6.0
	Antivirus
	Microsoft Word 2003 or newer (required to view pre-filled templates from VESTA)
	Microsoft .NET 2.0 framework (required to run VESTAdocup and VESTAcard)
Connectivity:	384bps internet connection

Recommended system requirements:

Hardware:	Dual-core processor (Intel Core 2 Duo, AMD Athlon x2)
	2 GB RAM
	SXGA (1280 x 1024) or WXGA (1280 x 768) display
Software:	Windows 7/8
	Microsoft Internet Explorer 8.0
	Antivirus
Connectivity:	1.5mbps (or better) internet connection