State of Nevada
HOMELESS MANAGEMENT INFORMATION SYSTEM
(HMIS)
Standard Operating Procedures

Section 1: Contractual Requirements and Roles

Bitfocus, Inc. Contractual Requirements: Bitfocus, Inc. ("Bitfocus"), in its role as Nevada HMIS System Administrator, agrees to use its reasonable best efforts to provide all of the necessary equipment and staff to operate and maintain the HMIS database. In addition, Bitfocus will provide technical assistance related to the use of Clarity Human Services software, relevant hardware, and adherence to HMIS policies and procedures, including HUD requirements, to all participating housing and services providers (the "Partner Agencies"). Additional services may be provided on a case-by-case basis, as agreed upon by Bitfocus and a Partner Agency.

Central Server Requirements: Security of equipment and data is a priority for Bitfocus. This document outlines the foundation for system security including the usage policy for access to the system, the data for export, import or data analysis needs, and physical system access, as well as the procedures for maintaining the system and data integrity.

HMIS Working Group: The Nevada HMIS has a Working Group to govern the project. The group is composed of representatives of stakeholders. This includes consumers, HUD funded agencies, homeless service agencies, local governments, and state government. Members of the Working Group will be elected from time to time by majority vote of all participating agencies. The qualifications and meetings of members of the Working Group and all other matters relating to the Working Group shall be provided in by-laws of the Working Group adopted or modified from time to time by majority vote of all of the participating agencies.

Central Server Management: Management of a HMIS requires several skill sets. The Working Group has identified the following roles to provide the best and most efficient service to HMIS stakeholders:

- *Systems Administrator* - assigns rights for users, merges duplicate files, manages maintenance reporting, backups, security, updates policy and procedures, monitors login attempts, completes system updates, approves any changes to the system, maintenance and disaster planning, and supervision of personnel.
- *Report Writer/Technical Assistant/Help Desk Support* - assists in the design of reports as needed by Partner Agencies and community stakeholders, answers user questions and assists users in resolving problems, if needed go onsite to resolve hardware/software issues.

As the user-base grows, it is understood that these positions and roles will be re-evaluated to meet the needs of stakeholders, as funding is available.

New Agency Contractual Requirements: Any agency wishing to participate in the Nevada HMIS must assume a share of all operational and acquisition costs for hardware, software and technical assistance to support the operation and maintenance of the

system. If Bitfocus is able to secure additional funding, these costs may be reduced or eliminated accordingly. In addition, all agencies requesting to participate in the HMIS must execute a Partner Agency MOU and Data Sharing Agreement.

The roles of every Partner Agency are defined in order to prevent confusion regarding responsibilities and privileges. The following roles must be filled in order for an agency to begin working with the project:

- Partner Agency Director
- Partner Agency HMIS Lead
- Partner Agency Technical Administrator
- Partner Agency Intake Worker or Case Manager

In addition, some Partner Agencies may also have the following roles:

- Partner Agency Mental Health Worker
- Partner Agency Substance Abuse Counselor
- Partner Agency Health Worker
- Partner Agency User
- Partner Agency Data Analyst
- Continuum of Care Representative

Note: In some cases, more than one role will be assigned to the same individual.

Partner Agency Director: Has access to all files and data regarding all programs and services operated by his or her agency.

Partner Agency HMIS Lead: Is the primary point of contact between Bitfocus and the Partner Agency.

Participating Agency Technical Administrator: Is able to edit, create, and append data for all programs and services operated by his or her agency; and is able to run reports regarding agency programs and services.

Participating Agency Intake Worker: Is able to create client files and run reports against the data collected at their agency; able to update and append client records; and able to view sensitive portions of the record if the client has consented and signed a release.

Participating Agency Case Manager: Is able to create client files and run reports against the data collected at their agency; able to update and append client records; and able to view sensitive portions of the record if the client has consented and signed a release.

Participating Agency Mental Health Worker: Is able to create client files and run reports against the data collected at their agency; able to update and append client records; and able to view sensitive portions of the record if the client has consented and signed a release.

Participating Agency Substance Abuse Counselor: Is able to create client files and run reports against the data collected at their agency; able to update and append client records; and able to view sensitive portions of the record if the client has consented and signed a release.

Participating Agency Health Worker: Is able to create client files and run reports against the data collected at their agency; able to update and append client records; and able to view sensitive portions of the record if the client has consented and signed a release.

Participating Agency Data Entry Worker: Is able to complete data entry only. Will not be able to view information after the information has been entered.

Participating Agency Data Analyst: Is able to view global reports regarding homeless persons in our community, demographics, service utilization, total statistics and numbers regarding persons in the system.

Regional Homeless Coordinator: Is able to view aggregate-level reports regarding our community, demographics, service utilization, total statistics and numbers regarding data in the system.

All users of the system should recognize that rights are assigned on a need to know basis.

Section 2: Participation Requirements

Participation Requirements: For most efficient utilization of the services provided by the HMIS, several steps must be completed at the agency level before implementation can begin. Although the System Administrator can assist with most steps, agencies should be prepared to act without assistance. These steps include:

- Acquisition of High Speed Internet Connectivity with at least one static IP address
- Identification of an on-site Technical Administrator to serve as the primary contact, or the name of an outside contractor.
- Completed network and security assessment to comply with the most recent version of the U.S. Department of Housing and Urban Development's (HUD's) HMIS rule, and /or HUD's HMIS Data Standards, and/or HUD's Continuum of Care Program Rule, as applicable
- Signing and executing a Partner Agency MOU and Data Sharing Agreement or other applicable agreement(s)
- Adopting written procedures concerning client consent for release of information, client grievance procedures and interview protocols as specified in this document.

Implementation Requirements: Partner Agencies must generate or obtain documents that cover each of the following areas in order for implementation to begin.

Written Client Consent for Data Entry: Partner Agencies must obtain the client's informed written consent prior to entering identifying information concerning a client into the system. If a client does not consent, services should not be denied to the client. The agency can use the anonymous client function in appropriate cases.

Confidentiality and Consent Forms: Partner Agencies must use the forms approved by the HMIS Working Group. Partner Agencies that share protected health information must have internal procedures for obtaining client consent prior to the sharing of this information.

Privacy Notice: Partner Agencies must develop a privacy notice, and incorporate the privacy notice into their policies and procedures. In addition, HUD mandates that organizations develop policies and procedures to distribute privacy notices to their employees, which include having employees sign to acknowledge receipt of the notices.

Interview Protocols: Each Partner Agency must develop a written program specific interview guide that includes the minimal data elements and any additional elements the agency wishes to collect.

Background Check Procedures: Each Partner Agency is responsible for conducting its standard employment background check for any employee, contractor, or volunteer who will use the HMIS.

Staff Confidentiality Agreements: Each Partner Agency must develop a procedure for informing staff of client confidentiality. All users of the system must complete general Clarity Human Services user training prior to being authorized to use the system. In addition, all users of the system are required to attend confidentiality and privacy training.

Information Security Protocols: Internal policies must be developed at each Partner Agency to establish a process for the detection and prevention of a violation of any HMIS information security protocols.

Virus Prevention, Detection, and Disinfection Protocols: Participation in the HMIS requires that Partner Agencies develop procedures intended to assure that computers with access to the system run updated anti-virus software.

Data Collection Commitment: Participation in the HMIS requires that all Partner Agencies collect minimum data elements on all consenting clients in accordance with HUD requirements.

Connectivity: Once implementation has begun each Partner Agency agrees to use its reasonable best efforts to maintain appropriate Internet connectivity in order to continue participation.

Maintenance of Onsite Computer Equipment: Each Participating Agency agrees to use its reasonable best efforts to maintain computer equipment to the extent required to continue participation.

Conversion of Legacy Data or Links to Other Systems: Partner Agencies that are using other systems or wish to have legacy data converted must provide resources and processes that enable conversion without cost to Bitfocus or the HMIS.

Section 3: Training

Administrator and Security Training: Bitfocus has provided training to instruct the System Administrator in the proper procedures to supervise and maintain the operation of the HMIS. System Administration training has covered security, configuration and user customization.

End User Training Schedule: Bitfocus will provide training in the day-to-day use of the HMIS on a regularly scheduled weekly or as needed basis. Training will use an established demo database, covering the following topics: intake, assessment, information and referral, security, reports, and client tracking. Training on any agency-modified fields/screens will be the responsibility of the agency making the modification. Bitfocus will also provide training about each user's responsibility to protect client privacy and ensure that basic system security is maintained, such as logging out of HMIS when it is not in use and maintaining password security. Users will not be provided access to the system without verification of training attendance.

Section 4: User, Location, Physical and Data Access

Access Privileges to the HMIS: Access to system resources will only be granted to Partner Agency staff that needs access in order to perform their duties.

Access Levels for HMIS Users: Each user of the system will be assigned an account that grants access to the specific system resources that he or she requires. A model of least-privilege is used; no user will be granted more than the least amount of privilege needed to perform his or her duties.

Access to Data: All data collected by the HMIS will be categorized. Access to data sets, types of data, and all other information housed as part of the HMIS is governed by policies approved by the HMIS Working Group and Bitfocus. Reproduction, distribution, destruction of and access to the data are based on the content of the data. At no time may identifying confidential data be distributed or accessible without the consent of the client.

Access to Client Paper Records: Partner Agency users should not have greater access to client information through the system than is available through the agency's paper files.

Physical Access Control: The building containing the central server is secured through locked key access. The room housing the central server has keyed entry with access to keys limited to Bitfocus, Inc. staff only.

System access over wireless networks: Access to the HMIS over any type of public wireless network is discouraged. Public wireless networks are more susceptible to unauthorized access than private wireless networks. For private networks, only Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2) security protocols are allowed.

Connecting to the Clarity Human Services Application: Clarity Human Services provides three standard authentication methods to ensure secure authentication, and other identification and access management functions, including"

- Basic Authentication – User must provide login and complex password credentials
- IP Whitelist – User or Partner Agency must access the system through a pre-approved list of IP Addresses
- Personal PKI Certificate – User or Partner Agency must have a valid PKI certificate installed within their Browser to access the system.

The system administrator can fully administer each method of authentication.

Unique User ID and Password: Each user of the system must be individually and uniquely identified. Identification will be verified through a password. Users are not permitted to share their password or permit other users to log in to the system with their password. Passwords will be at least eight characters long and meet reasonable industry standard requirements. These requirements are:

1) Using a combination of at least 3 of the following:
   a. Numbers
   b. Lowercase letters
   c. Capital letters
   d. Special characters (e.g. ~ ! @ # $ % ^ & * ( ) _)
2) Not using, or including, the username, the HMIS name, or the HMIS vendor's name
3) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards

Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users will not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Right to Deny User and Participating Agencies' Access: The Working Group has the right to suspend, limit or revoke the access of any agency or individual for violation of HMIS policies. Upon remedy of said violation, access rights may be reinstated. If privileges have not been reinstated, the person or agency can file an appeal to the HMIS Working Group for reinstatement.

Monitoring: Access to the system will be monitored. In addition, the HMIS will maintain logs of all actions taken within the system including login transactions and detailed monitoring of user data transactions within the software. Bitfocus will use its best reasonable efforts to review logs on a regular basis. It is understood that agencies will cooperate with all monitoring requirements. All exceptions that show security policy violations will be investigated.

Data Integrity Controls: Access to the production data is restricted to essential system administrative staff only. Each staff member that has access to production data is contracted to not alter or impact the data in any adverse way.

Section 5: Technical Support and System Availability

Planned Technical Support: Bitfocus will use its reasonable best efforts to offer technical support to all Partner Agencies. Support services of the HMIS include: training, implementation support, report writing support, and process troubleshooting.

Partner Agency Service Requests: System administrative staff is only permitted to respond to service requests that are submitted in writing by the Partner Agency Executive Director, Technical Administrator, or designated HMIS Lead.

Rapid Response Technical Support: An emergency contact number will be provided for requests for service that require a rapid response (i.e., unable to access system). These service requests will be prioritized above other requests. Partner Agencies should plan accordingly.

Availability: The goal is to have the system available 24 hours a day, subject to scheduled outages for updating and maintenance. Bitfocus will use its reasonable best

efforts to achieve a 99% uptime. On occasion, there will be planned system outages. Partner Agencies will be notified a minimum of 48 hours before a planned but unscheduled outage is to occur. Bitfocus will use its reasonable best efforts to address unplanned interruptions within 24 hours, and agencies will be notified when the system becomes available.

Section 6: Stages of Implementation

Stage 1 – Startup: Partner Agencies must complete all MOUs and agreements, and adopt all policies and procedures required in this document.

Stage 2 – Organization Data Entry: Partner Agencies must define the organization and provide detailed descriptions of programs and eligibility, as well as define user workflow.

Stage 3 – Initial System Rollout: Partner Agencies must ensure that privacy and confidentiality training is completed for all users. They must also define users and responsibilities. All HMIS training must be conducted using a demonstration version of the software and data. Real client data will **NEVER** be used for training purposes.

Stage 4 – Client Data Entry: Partner Agencies must begin entering client information into the HMIS.

Stage 5 – Client-Program Entry: Partner Agencies must begin entering client use of their programs.

Stage 6 – Case Management: Partner Agencies may use the system as a case management tool in the day-to-day operation of the agency if the agency wishes to do so.

Stage 7 – Program Management: Partner Agencies may use the system to track program performance on an agency level.

Section 7: Encryption Management

Encryption General: All information should be encrypted in the database per HUD standards. All connections to the database should be encrypted to HUD standards or higher. Encryption should be sufficient to prevent unauthorized personnel from accessing confidential information for any reason.

Encryption Management: In the event that system wide data decryption becomes necessary, the Working Group must obtain the written authorization of every Partner Agency's Executive Director.

Section 8: Data Release Protocols

Data Entry: Before any data will be entered into the HMIS, the client must first consent to data entry and agree to what information can be entered into the system. Upon completion of the approved consent form, the Partner Agency will only enter the information into the system that has been approved by the client. The HMIS will assign

the client a unique personal identifier. Partner Agencies should note that services must not be contingent on a client consenting to data entry.

Anonymous Client Data Entry: In the event that a client does not want to have personally identifying information entered into the HMIS, he or she will be entered following the Anonymous Client Record Data Entry Protocol listed below:

Basic Anonymous Client Record Data Entry Protocol:

- Start with Quality of Name field and enter "Client Refused"
- Enter zeros for a SSN
- Change to "Client Refused" for Quality of SSN
- Type "Refused" for Last Name
- Type "Consent" for First Name
- Enter 01/01/ and estimate a year for Date of Birth (to determine an adult from a child)
- Enter "Approximate" for Quality of DOB
- Enter Gender, Race, Ethnicity, and Veteran status with real data if it won't serve to identify them in any way
- Leave Middle Name and Suffix blank
- Click Add Record
- Make note in the clients paper file of the unique identifier that is auto generated for this client as this will be the only means of finding this client via the search function for future service provisions

Sharing Protected Information: A Client Consent for Data Collection and Release of Information (ROI) document indicating what information the client agrees to have shared with other Partner Agencies should be signed prior to sharing of any Protected Personal Information ("PPI") including identifying information (such as the client's name, birth date, gender, race, social security number, phone number, residence address, photographic likeness, and other similar identifying information) and financial information (such as the client's employment status, income verification, public assistance payments or allowances, food stamp allotments, and other similar financial information). All ROI forms that were valid and officially approved for use by the HMIS Steering Committee at the time they are signed by a client will be accepted.

Printed Information: Printed records disclosed to the client or another party should indicate the identity of the individual and/or agency to whom the record is directed, the date, and the initials of the person making the disclosure.

Requests for HMIS Client Information: The Partner Agency must notify Bitfocus within one working day when the Partner Agency receives a request from any individual or outside organization for client-identifying information.

Case Notes: It is understood that client case notes will not be shared, and that each Partner Agency will have the ability to enter its own private notes about a client.

The Client Consent for Data Collection and Release of Information (ROI) form will be a dated document with a defined term. The Partner Agency will only be able to access the information specified on the form that was entered into the system during the time the form was in effect. Also, the client can revoke his or her consent at any time, in full or in part, and have his or her file deactivated, by signing a Client Revocation of Consent form or submitting a written and signed request to remove their consent. In emergency

situations, such as domestic violence, clients may revoke consent verbally to Partner Agency staff.

Section 9: Internal Operating Procedures

Computer Virus Prevention, Detection, and Disinfection: The goal of the system will be to incorporate and maintain updated virus protection from a reputable single source. Any and all viruses found will be quarantined and analyzed. If unrepairable, the virus will be deleted. Partner Agencies are required to run and maintain their own anti-virus software from an approved source on all computers that have access to the HMIS system.

Operating System Updates: The goal will be to update or patch the HMIS within a reasonable time after review of the vendor's release of updates and patches and approval by the system administrator.

Backup and Recovery: The goal will be to back up the system on a daily basis. Backup media will be stored in a fire-protected safe with the server. In addition, backups will be stored electronically, offsite. A backup of hardware and system software will be stored in an offsite location so that it will be available in the event of catastrophic failure.

Disaster Recovery Process: The goal will be to review disaster recovery processes and check offsite systems checked for viability twice per year.

Community Reporting Process: At the direction of the Working Group, Bitfocus will publish community-wide aggregate reports on the clients in the system on a periodic basis. These report(s) will reflect raw, point-in-time data.

Termination of the HMIS: In the event the HMIS ceases to exist, Partner Agencies will be notified and provided a reasonable time to access and save client data on those served by the respective agencies as well as statistical and frequency data from the entire system. Then, the information on the central server will be purged or stored. If the latter occurs, the data will remain in an encrypted and aggregate state.

Termination of Bitfocus as System Administrator: In the event Bitfocus is no longer the system administrator, custodianship of the data on the HMIS system will be transferred to the HMIS Working Group or to a successor system administrator, and all Partner Agencies will be informed in a timely manner.

Section 10: HMIS Client Grievance Procedures

If a client has any issue with the HMIS at a Partner Agency, the client should work with that agency to resolve the problem.

If the problem is still not resolved to the client's satisfaction, the client can request an 'HMIS Grievance Form' (blank copies of this form are available on the Nevada CMIS website – www.nvcmis.bitfocus.com). Specific instructions are listed on the form.

Bitfocus will receive the form, and will distribute copies to all Working Group Members. The Working Group will be notified of all grievances received. Bitfocus will use its best reasonable efforts to investigate the issue, and will inform the Working Group of the results.

If the issue is not system related, the Working Group will recommend the best course of action to handle the grievance.

Any material change(s) resulting from a grievance (system related or not) requires approval from the Working Group.

Section 11: HMIS Privacy Notice

An individual has a right to adequate notice of the uses and disclosures of protected personal information that may be made by a Partner Agency and of the individual's rights and the Partner Agency's legal duties with respect to protected personal information. The notice should be prominently displayed in the program offices where intake occurs. The Partner Agency should promptly revise and redistribute its notice whenever there is a material substantive change to the permitted uses or disclosures, the individual's rights, the Partner Agency's legal duties, or other privacy practices stated in the notice. Partner Agencies should maintain documentation of compliance with the notice requirements by retaining copies of the notices issued by them. A client has the right to obtain a paper copy of the notice from the Partner Agency upon request. An inmate does not have a right to notice, and the requirements of this notice do not apply to a correctional institution that is a system user.

Content of Notice: The Participating Agency must provide a notice that is written in plain language and that contains the elements required by this section. These elements are not exclusive, and either oral or written notice may inform the individual of the permitted uses of information. The following statement as a header or otherwise must be prominently displayed: ''THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.''

- A description of each of the purposes for which a Partner Agency is permitted or required by this notice to use or disclose protected personal information without the individual's written consent or authorization. These include administrative, programmatic, and academic research purposes.

- If a use or disclosure is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law.

- A statement that consensual uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization.

- A statement of the individual's rights with respect to protected personal information and a brief description of how the individual may exercise these rights.

- A statement that the Partner Agency is required by law to maintain the privacy of protected personal information and to provide individuals with notice of its legal duties and privacy practices with respect to protected personal information.

- A statement that the Partner Agency is required to comply with the terms of the notice currently in effect.

- A statement that reserves the right to change the terms of the notice and to make the new notice provisions effective for all protected personal information. The statement must also describe how the Partner Agency will attempt to provide individuals with a revised notice.

- A statement that individuals may complain to the Partner Agency if they believe their privacy rights have been violated.

- A brief description of how the individual may file a complaint with the Partner Agency.

- A statement that the individual will not be retaliated against for filing a complaint.

- The name, or title, and telephone number of a person or office to contact for further information.

- The date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published

Section 12: Participation without using Clarity Human Services software (data feeding)

If a Partner Agency wishes to participate in the HMIS, but does not wish to use the Clarity Human Services software, the following additional guidelines must be met:

1) Partner Agency understands that it is its responsibility to pay for any additional costs related to feeding data to the HMIS.
2) Partner Agency must be able to produce an extract file from its existing system.
3) Partner Agency must be able to produce the extract file in a format specified by Bitfocus that meets the most current HUD requirements.
4) Partner Agency understands that the extract format will most likely change in the future due to HUD standardized import file format specifications.
5) Partner Agency data imported into the HMIS will be available only for the purpose of generating aggregate reports.
6) If, at a later date, an agency chooses to use the Clarity Human Services software, the agency understands that its historical imported data will not be available.
7) Sections 1 – 8 of this document do not apply to agencies feeding data to the HMIS.

Section 13: Sharing data between agencies

If a Partner Agency wishes to share data through the HMIS with one or more other agencies:

1) All Partner Agencies wishing to share data must meet with Bitfocus to discuss and address all details of data sharing. For example: What information is to be shared, direction of sharing, etc.
2) A separate Memorandum of Understanding must be created between Bitfocus and all Partner Agencies that will participate in the inter-agency sharing.
3) Partner Agencies must comply with Section 8 of this document (relating to obtaining clients' permission to have their information shared).

Section 14: User Meetings

User meetings will be scheduled periodically with advance notice given via the HMIS mailing list and posted on the system login screen. The Bitfocus staff responsible for HMIS matters should be available to confer with Partner Agencies via phone, e-mail or in person.

While most meetings will be optional to attend, it may be necessary to request mandatory attendance at a particular meeting. If this becomes necessary, ample notice will be given.

Section 15: Guidelines on Removing Agencies or Users

Voluntary Removal: If a Partner Agency or user no longer wants to access the system, they simply need to contact Bitfocus and inform them of the decision. In the case of user removal, it is the relevant Partner Agency's responsibility to contact Bitfocus in a timely fashion so the User ID can be deactivated to prevent unauthorized access to the system. A Partner Agency asking to be removed from the system understands the following:

1) The Partner Agency will receive one (1) copy of the data it has input into the system. This copy will be in a format determined by Bitfocus and approved by the Working Group. The Partner Agency will be given an appropriate description of the data format.
2) The data the Partner Agency enters into the system will remain in the system for the purposes of producing aggregate non-identifying reports. Any Partner Agency information will remain in the system, but will be marked as inactive.
3) The Partner Agency must return all hardware (firewalls, etc.) that are owned by Bitfocus.
4) Any fees paid for participation in the HMIS will not be refunded.
5) The Partner Agency understands and accepts any ramifications for not participating in the system.

Involuntary Removal: It is vital for the Working Group and Bitfocus to provide a secure service for all users. Any action(s) that threaten the integrity of the system will not be tolerated.

1) Bitfocus reserves the right to modify, limit and/or suspend any user account at any time if there is a security risk to the system
2) Any improper use of the system is subject to immediate suspension of the user's account. The penalties imposed on a user for improper system use will vary based on the level of the offense. Typically the user will receive a warning on the first offense. However, if the offense is severe enough, Bitfocus reserves the right to disable the account immediately and in extreme cases, may disable all users' access by the Partner Agency in question.
3) Bitfocus will contact the organization within one business day of any suspension.
4) If a users account is suspended, only the Executive Director or designated HMIS Lead for a Partner Agency may request account re-activation. Suspended users may be required to attend additional training before having their access reinstated.
5) In the event that a Partner Agency is removed from the system they must submit a written request for reinstatement to the Working Group and Bitfocus. If a Partner Agency is not reinstated into the system after review, the Partner Agency

will be given one (1) copy of its data in a format that will be determined by Bitfocus and approved by the Working Group (the Partner Agency will also be provided with a description of the data format). Data will not be given to the Partner Agency until all hardware (firewalls, etc.) belonging to Bitfocus are returned. Any fees paid for participation in the system will not be returned.

6) All system users agree to waive and release any and all claims and expenses related to or arising from the user's violation of this agreement against the Working Group, the employers of the respective members of the Working Group, Bitfocus, its officers, directors, shareholders, employees, agents, subsidiaries and affiliates.

Section 16: Additional Participation Standards

System/Data Security: In the event a Partner Agency becomes aware of a system security or client confidentiality breach, the Executive Director of the Partner Agency shall notify Bitfocus of the breach within one business day.

HMIS related forms and printed material: The Partner Agency agrees to maintain all Client Authorization and/or Release of Information forms related to the HMIS. This information may be requested by the Working Group, Bitfocus, and/or its contractors for periodic audits.

Destruction of HMIS related printed material: Any HMIS forms or printed information obtained by a Partner Agency or user from the HMIS must be destroyed in a manner that ensures client confidentiality will not be compromised.

Section 17: No Third Party Beneficiaries

The foregoing operating procedures have been set forth solely for the benefit and protection of the Working Group, Bitfocus and the respective Partner Agencies and their respective heirs, personal representatives, successors and assigns. No other person or entity shall have any rights of any nature in connection with or arising from the foregoing operating procedures or by reason hereof. Without limiting the generality of the preceding sentence, no user of the HMIS in his or her capacity as such and no current, former or prospective client of any Partner Agency shall have any rights of any nature in connection with or arising from the foregoing operating procedures or by reason hereof.

Section 18: HMIS Concepts and Terms

Aggregate - Collected together from different sources and considered as a whole, and lacking identifying information.

Client - Somebody who uses or applies to use the services of a participating agency.

CoC - The acronym for Continuum of Care

Community - A group of people with a common background or with shared interests within a defined geographic area, for our area to include the State of Nevada.

Confidentiality - Entrusted with somebody's personal or private information or matters.

Connectivity – The ability to connect two or more systems together. Pertaining to the HMIS, the use of a high speed Internet connection for accessing the system.

Consent – Express acceptance of or agreement to something.

Data – The information in the system, for example, numbers, text, images, and sounds, in a form that is suitable for storage in or processing by a computer

Decryption – To render an encoded amount of data into plain language or out of its encrypted state.

Encryption – To convert computer data and messages to something incomprehensible by means of a key, so that only an authorized recipient holding the matching key can reconvert it.

Firewall – A component of a network that prevents unauthorized users and/or data from getting in or out of the network, using rules to specify acceptable communication

HMIS – The acronym for Homeless Management Information Systems, sometimes also referred to as HIMS or Homeless Information Management System.

HUD – The acronym for the Department of Housing and Urban Development.

Legacy Data – Information stored in an older version of software or format that is not compatible with the HMIS.

Clarity Human Services– The name of the software application that is being used for the Nevada HMIS.

MOU – The acronym for Memorandum of Understanding. A document that outlines the specific areas of agreement between two or more parties.

Organization - A group of people identified by shared interests or purpose.

PPI – The acronym for Protected Personal Information.

Program – A collection of services grouped together.

ROI – The acronym for Release of Information.

Service - The system or operation by which people are provided with something.

VPN – The acronym for Virtual Private Network. A way for securely connecting systems together to transmit data.