



## **King County Homeless Management and Information System (HMIS) PARTNER AGENCY TECHNICAL ADMINISTRATOR AND SECURITY OFFICER AGREEMENT**

This Agreement is entered into by and between King County Regional Authority on Homelessness (“KCRHA”) and the undersigned parties in order to establish the responsibilities described herein and to confirm compliance with required background check requirements as set forth below. KCRHA reserves the right to request access to the Partner Agency records and place of business for monitoring compliance with this Agreement.

The King County Homeless Management Information System (“HMIS”) is a shared database and software application which confidentially collects, uses, and shares client-level information related to homelessness in King County. On behalf of the King County Continuum of Care (“CoC”), HMIS is administered by KCRHA and Bitfocus, Inc. (“Bitfocus”) in a software application called Clarity Human Services (“Clarity”).

Clients must consent to the collection, use, and release of their information, which helps the CoC to provide quality housing and services to homeless and low-income people. Client information is collected in HMIS and released to housing and services providers (each, a “Partner Agency,” and collectively, the “Partner Agencies”), which include community-based organizations and government agencies. Partner Agencies use the information in HMIS: to improve housing and services quality; coordinate referral and placements for housing and services; to identify patterns and monitor trends over time; to conduct needs assessments and prioritize services for certain homeless and low-income subpopulations; to enhance interagency coordination; and to monitor and report on the delivery, impact, and quality of housing and services.

Pursuant to the HMIS Standard Operating Policies and the HMIS Security Plan, each HMIS Partner Agency must designate a technical administrator, also referred to as the HMIS Agency Lead, (the “Partner Agency Technical Administrator”) and a security officer (the “Partner Agency Security Officer”) to fulfill the responsibilities enumerated below. Furthermore, the Partner Agency Technical Administrator and the Security Officer may be the same person.

The **Partner Agency Technical Administrator** is responsible for:

- Overseeing the Partner Agency's compliance with the most recent versions of the Partner Agency Privacy and Data Sharing Agreement and Memorandum of Understanding and all other applicable plans, forms, manuals, standards, agreements, policies, and governance documents;
  - Detecting and responding to violations of any applicable HMIS plans, forms, manuals, standards, agreements, policies, and governance documents;
  - Serving as the primary contact for all communication related to the HMIS at the Partner Agency and forwarding such information to all Partner Agency authorized agents and representatives ("HMIS End Users," or simply "End Users") as she or he deems appropriate;
  - Ensuring complete and accurate data collection by Partner Agency End Users as established by HMIS plans, forms, manuals, standards, agreements, policies, and governance documents;
  - Providing first-level End User support;
  - Requesting End User account access;
  - Ensuring the Partner Agency maintains adequate internet connectivity;
  - Maintaining complete and accurate Partner Agency and program descriptor data in HMIS;
  - Working with Bitfocus to configure provider preferences (including assessments, referrals, services, etc.) in HMIS;
  - Completing agency-level reporting and/or supporting agency programs according to applicable reporting standards established by the U.S. Department of Housing and Urban Development ("HUD") and local funders; and ●
- Performing authorized imports of client-level data.

The **Partner Agency Security Officer** is responsible for:

- Conducting a complete and accurate semi-annual review of the Partner Agency's compliance with all applicable plans, forms, manuals, standards, agreements, policies, and governance documents;
- Completing the HMIS Semi-Annual Compliance Certification Checklist (the "Checklist"), and forwarding the Checklist to the HMIS System Administrator, as defined therein;
- Continually monitoring and maintaining security of all staff workstations and devices used for HMIS data entry which includes, but is not limited to, ensuring workstation computers are password-protected and locked when not in use, ensuring that nonauthorized persons are unable to view any HMIS workstation computer monitor, and ensuring that documents printed from HMIS are sent to a printer in a secure location where only Authorized Persons have access;

- Safeguarding client privacy by ensuring Partner Agency and Partner Agency End User compliance with all HUD Rules;
- If Agency agrees to allow access to HMIS from agency computers and Portable Electronic Devices, assure compliance with the HMIS Partner Agency Privacy and Data Sharing Agreement standards.
- Investigating potential and actual breaches of either HMIS system security or client confidentiality and security policies, and immediately notifying the KCRHA and the System Administrator, as defined in the Checklist, of substantiated incidents;
- Developing and implementing procedures for managing new, retired, and compromised local system account credentials;
- Developing and implementing procedures that will prevent unauthorized users from connecting to any private Partner Agency networks;
- Ensuring all Partner Agency End Users sign and execute the HMIS End User Agreement; and
- Ensuring all Partner Agency End Users complete the required New User General Training, and Annual Security and Privacy Training, as well as all other mandatory trainings; retaining documentation of training completion; and forwarding such documentation to the HMIS System Administrator.

As required by HUD, the Partner Agency shall perform a background check on any End User who is:

- Designated as a Partner Agency Technical Administrator, ● Designated as a Partner Agency Security Officer, or ● Granted agency manager-level access in HMIS.

The Partner Agency Executive Director shall ensure that such background checks are completed and shall approve the results before the End User is (i) granted a Technical Administrator or Security Officer title, or both, as applicable, or (ii) granted agency manager-level access in HMIS. The results of the background check shall be retained by the Partner Agency in the End User's personnel file. A background check may be conducted once for each End User unless otherwise required.



## **King County Homeless Management and Information System (HMIS)**

# PARTNER AGENCY TECHNICAL ADMINISTRATOR AND SECURITY OFFICER AGREEMENT

Partner Agency Name: \_\_\_\_\_

On behalf of the Partner Agency, I will be fulfilling the role of (check all that apply):

- Partner Agency Technical Administrator
- Partner Agency Security Officer

By signing, I agree to fulfill all of the responsibilities enumerated above for my role.

\_\_\_\_\_  
HMIS End User Printed Name

\_\_\_\_\_  
HMIS End User Signature

\_\_\_\_\_  
Date

I certify that a background check has been completed on the End User named above, that I approve the results, and that a copy of the results is filed with the End User's personnel file.

Further, I certify that Partner Agency will ensure the End User named above performs each of these functions.

\_\_\_\_\_  
Partner Agency Executive Director Printed Name

\_\_\_\_\_  
Partner Agency Executive Director Signature

\_\_\_\_\_  
Date