SANTA CLARA COUNTY HMIS
PARTNER AGENCY TECHNICAL ADMINISTRATOR
AND SECURITY OFFICER AGREEMENT

The Santa Clara County Homeless Management Information System ("SCC HMIS") is a shared database and software application which confidentially collects, uses, and shares client-level information related to homelessness in Santa Clara County. On behalf of the Santa Clara County Continuum of Care ("CoC"), SCC HMIS is administered by the County of Santa Clara ("County") 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 SCC HMIS and released to housing and services providers (each, a "Partner Agency," and collectively, the "Partner Agencies"), which includes community based organizations and government agencies. Partner Agencies use the information in SCC HMIS: to improve housing and services quality; to identify patterns and monitor trends over time; to conduct needs assessments and prioritize services for certain homeless and low-income subpopulations; to enhance inter-agency coordination; and to monitor and report on the delivery, impact, and quality of housing and services.

Pursuant to the SCC HMIS Standard Operating Procedures and the SCC HMIS Security Plan, each HMIS Partner Agency must designate a technical administrator (the "Partner Agency Technical Administrator") and a security officer (the "Partner Agency Security Officer") to fulfill the responsibilities enumerated below.

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 SCC HMIS plans, forms, manuals, standards, agreements, policies, and governance documents;
- Serving as the primary contact for all communication related to the SCC HMIS at the Partner Agency and forwarding such information to all Partner Agency authorized agents and representatives ("SCC 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 SCC HMIS plans, forms, manuals, standards, agreements, policies, and governance documents;
- Providing first-level End User support;
- Requesting End User licenses;
- Ensuring the Partner Agency maintains adequate internet connectivity;

- Maintaining complete and accurate Partner Agency and program descriptor data in SCC HMIS;
- Working with Bitfocus to configure provider preferences (including assessments, referrals, services, etc.) in SCC 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
- Performing authorized imports of client-level data.

The Partner Agency Security Officer is responsible for:

- Conducting a complete and accurate quarterly review of the Partner Agency's compliance with all applicable plans, forms, manuals, standards, agreements, policies, and governance documents;
- Completing the SCC HMIS Quarterly Compliance Certification Checklist (the "Checklist"), and forwarding the Checklist to the HMIS Lead Agency and the System Administrator, as defined therein;
- Continually monitoring and maintaining security of all staff workstations used for SCC HMIS data entry;
- Safeguarding client privacy by ensuring Partner Agency and Partner Agency End User compliance with all applicable confidentiality and security policies;
- Investigating potential and actual breaches of either SCC HMIS system security or client confidentiality and security policies, and immediately notifying the County 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 SCC HMIS End User Agreement and retaining records of all signed SCC HMIS End User Agreements; and
- Ensuring all Partner Agency End Users complete the SCC HMIS Privacy and Security Training, SCC HMIS Client Consent Training, and the SCC HMIS Workflow Training, as well as all other mandatory trainings; retaining documentation of training completion; and forwarding such documentation to the HMIS Lead Agency.

The Partner Agency must perform a background check on any End User:

- Designated as a Partner Agency Technical Administrator,
- Designated as a Partner Agency Security Officer, or
- Granted administrator-level access in SCC HMIS.

Such background check must be completed and the results approved by the Partner Agency Executive Director before the End User is (i) granted with a Technical Administrator or Security Officer title, or both, as applicable, and (ii) granted administrator-level access in SCC HMIS. The results of the background check must 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.

Partner Agency Name: _____

SCC HMIS End User 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.

_____ _____
SCC HMIS End User Signature Date

(To be completed by the Partner Agency Executive Director)
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