AGENDA REPORT

CITY OF OAKLAND

TO: Edward D. Reiskin City Administrator	**FROM:** Guillermo Cespedes Chief, Violence Prevention
SUBJECT: DVP Data Management System – SUPPLEMENTAL Report	**DATE:** July 5, 2022

City Administrator Approval _[signature]_   Date: **Jul 7, 2022**

RECOMMENDATION

Staff Recommends That The City Council Adopt A Resolution (1) Authorizing The City Administrator To Waive the Local and Small Local Business Enterprise Program (L/SLBE) and the Competitive Bidding Process and Award a Five-Year Contract, From August 1, 2022 To June 30, 2027, To Social Solutions Global, Inc. For The Development Of An Apricot 360 Data Management System and For Annual Licensing And Technical Assistance Fees For a Total Amount Not To Exceed Five Hundred Thirty-Three Thousand Fifty-Six Dollars ($533,056); And (2) Adopting The Surveillance Use Policy Attached Hereto As Exhibit A Pertaining To The Apricot 360 Data Management System.

REASON FOR SUPPLEMENTAL REPORT

At the Public Safety Committee meeting on April 12, 2022, the DVP presented its request for City Council to approve a contract between the City of Oakland and Social Solutions Global, Inc. to create and maintain a new data management system (Apricot 360) for the Department of Violence Prevention (DVP). The request for a new data management system responds to years of feedback from DVP grantees about challenges with the existing Cityspan system, and it reflects a greater need for data collection and oversight resulting from an increased investment from City Council in violence prevention and intervention services. At the meeting on April 12, 2022, the Committee approved the item (Subject: *DVP Data Management System*) for inclusion on the City Council consent calendar but requested that the DVP first present the item to the Privacy Advisory Commission (PAC).

DVP staff prepared the required impact report and use policy for the Apricot 360 data management system and presented at the May 5, 2022, regularly-scheduled meeting of the PAC. The PAC indicated support for the DVP's Apricot 360 Impact Report and Use Policy but requested to review a draft contract between the City of Oakland and Social Solutions Global, Inc. prior to taking a vote. The DVP provided the draft contract to Chair Brian Hofer on May 9, 2022, and Chair Hofer convened a special meeting of the PAC on May 18, 2022. At the May 18th special meeting, several commissioners expressed concern regarding the need for select

City Council
July 19, 2022

DVP staff to have access to individual-level client records and personally-identifiable information (PII; defined as full names and dates of birth). Commissioners also had a number of additional questions pertaining to system security and data access. The PAC declined to vote on the submitted use policy at that meeting and rescheduled the item for the regularly-scheduled June 2, 2022, meeting agenda. Prior to the June 2, 2022, meeting, DVP staff revised the Apricot 360 Impact Report and Use Policy, as well as the contract between the City of Oakland and Social Solutions Global, Inc., to address and clarify the questions raised by commissioners. DVP staff received the feedback from Chair Hofer indicating an intention to approve the revised Apricot 360 Use Policy at the meeting on June 2, 2022, based on the revisions that had been made.

At the meeting on June 2, 2022, Vice Chair Lou Katz and representatives from three DVP-funded organizations (Youth ALIVE!, Family Violence Law Center, and Youth Employment Partnership) spoke against the DVP's access to any individual-level client records or PII through the Apricot 360 system. Additionally, several additional concerns were raised by commissioners relating to the contract documents. As a result, the PAC declined to vote on the Apricot 360 Use Policy again and added it to the agenda for their regularly-scheduled meeting on July 7, 2022.

ANALYSIS/POLICY ALTERNATIVES

As of this writing on July 5, 2022, the DVP has developed and submitted two different Apricot 360 Use Policies (attached to this report as **Attachments A and B**) to the PAC for review and discuss at the meeting on July 7, 2022. Version A of the Apricot 360 Use Policy (**Attachment A**) preserves access to individual-level client records and PII for a limited number of DVP staff for the DVP's group and gun violence strategy. Staff's rationale for needing access to this data is provided in greater detail below. Version B of the Apricot 360 Use Policy (**Attachment B**) removes all access to individual-level client records and PII from DVP staff so that DVP staff only have access to aggregate-level service delivery data for the group and gun violence strategy. In both versions of the use policy, DVP staff do not have access to individual-level client records or PII for the gender-based violence (GBV) or community healing strategies. This information is not required for the GBV strategy due to Violence Against Women Act (VAWA) privacy regulations that prevent GBV agencies from sharing that information. This information is also not needed for the community healing strategy due to the fact that the majority of activities within the community healing strategy are group activities for which individual-level data are not practical (e.g. Town Nights, mini grants, etc.).

The DVP's expectation is that the PAC will vote on July 7, 2022, to approve Version B of the Apricot 360 Use Policy (Attachment B). The DVP, however, is recommending that City Council adopt Version A of the Apricot 360 Use Policy (**Attachment A** to the report and **Exhibit A** to the resolution), which includes permission for a limited number of DVP staff to access to individual-level client records and PII for the group and gun violence strategy: (1) senior staff who coordinate the DVP's violent incident crisis response work, and (2) staff who perform data and evaluation functions. Explanations for the need for data access by these two groups is provided below, and **Table 1** details requirements for data entry and data visibility by activity within the group and gun violence strategy.

1) ***Senior staff within the DVP who coordinate the City's 24/7 violent incident crisis response*** require access to individual-level client records and PII to ensure that responses to shootings and homicides, which often involve activities performed by multiple agencies, are performed in a timely manner with high levels of communication

and coordination between agencies to reduce the likelihood of retaliation and ensure that victims and families receive needed services. For instance, violence interrupters from multiple agencies may respond to a single shooting or homicide incident due to the location of the incident or relationships with the individuals involved. Information on conversations with family members and associates of the victim that are documented in Apricot 360 can then be referenced by senior DVP coordination staff to ensure that adequate communication and coordination across agencies is taking place to minimize the likelihood of retaliation. For the same incident, the victim or family might be referred to one organization for relocation services and another organization for family support services, which should also be closely monitored by the DVP to ensure high levels of responsiveness. Lack of access to individual-level client information and PII by senior violent incident crisis response staff within the DVP would significantly limit the city's ability to effectively prevent future violence in response to shootings and homicides.

2) ***Data and evaluation staff within the DVP*** also require access to individual-level client records and PII for group and gun violence substrategies for the following reasons:
   a. Client accountability: It is possible that the same client might enroll in life coaching or employment services provided by different CBOs at the same time, which limits the availability of services and financial incentives for other clients. With access to PII, DVP staff will be able to easily flag duplicate enrollments and ensure that clients are only being served by one provider of a specific service type at a time. Without access to PII, DVP staff are unable to know whether the same client is receiving the same services from multiple agencies at once.
   b. Service delivery accountability: With access to PII, DVP staff will be able to periodically verify that services are being delivered to clients in accordance with service delivery data being entered into Apricot 360. DVP staff will also be able to ensure that CBOs are meeting their contract deliverables in terms of numbers of clients served through unique client enrollments rather than repeated or ongoing enrollment of the same clients.
   c. Ongoing process evaluation: DVP data and evaluation staff will be able to periodically review client data to determine the frequency and quality of services being rendered to ensure that they comply with DVP service delivery models. DVP staff will also be able to easily understand and describe the population of individuals accessing services funded by the DVP and their patterns of service enrollment, uptake, dropout, completion, reenrollment, etc.
   d. Data entry technical support: With access to individual-level records, DVP data and evaluation staff will be able to help grantees troublesohot any data entry challenges they encounter without soliciting support from the Apricot 360 technical support team.

Table 1. Entry and visibility of individual client records and PII for the DVP's group and gun violence strategy.

Substrategy	Activity	Are individual client records entered?	Is PII entered?	Are individual records and PII visible to DVP staff?
Employment & Education Support Services	Adult employment & education services	Yes	Yes	Yes
	Youth job exploration & education services	Yes	Yes	Yes
School Site Violence Intervention & Prevention Teams	Community healing	No	No	No
	Gender-based violence: Individual-level services	Yes	Provider choice	No
	Gender-based violence: Group services	No	No	No
	Violence interruption	Yes	Yes	Yes
	Youth Life Coaching	Yes	Yes	Yes
Violent incident crisis response	Emergency relocation	Yes	Yes	Yes
	Family support following homicide	Yes	Yes	Yes
	Hospital intervention	Yes	Yes	Yes
	Violence interruption	Yes	Yes	Yes
Youth Diversion and Youth & Adult Life Coaching	Adult life coaching	Yes	Yes	Yes
	Housing-focused case management	Yes	Yes	Yes
	Youth diversion: Individual-level services	Yes	Yes	Yes
	Youth diversion: Group-level services	No	No	No
	Youth life coaching	Yes	Yes	Yes

After an extensive review of the Health Insurance Portability and Accountability Act (HIPAA), in consultation with legal experts, the DVP has determined that information requested from funded-CBOs for group and gun violence substrategies does not constitute a breach of HIPAA. DVP staff have also not identified any legal prohibitions related to the collection of juvenile data required for the youth life coaching, youth diversion, and school-based substrategies.

Findings Required by Municipal Code Section 9.64.030(2)(B)
CitySpan, the DVP's current data management system vendor, does not provide the functionality that the DVP needs to comprehensively monitor and coordinate services provided to clients by DVP grantees.

The Apricot Use Policy will safeguard civil liberties and civil rights by allowing staff access to data records only on a need-to-know and right-to-know basis meaning that they will only have access to data that is essential to their job function. Apricot 360 allows administrators to restrict access to client records and individual fields within client records for staff members based on their pre-determined access requirements. Unauthorized use of the system by any staff person with any level of access will lead to disciplinary action, which could include termination of a

service provider's grant agreement and cessation of funding and, with respect to City employees, discipline up to and including termination. The Apricot 360 software meets current Housing and Urban Development Domestic Violence, Homeless Management Information System, and Social Security Administration data management and security protocols, as well as minimum required Family Educational Rights and Privacy Act (FERPA) and HIPAA standards. Additionally, all staff who access the Apricot 360 system will first be extensively trained by Apricot 360 trainers and/or the DVP's data and evaluation staff, and they will be trained in the DVP's Apricot 360 Surveillance Use Policy.

DVP staff evaluated the proposals submitted by Salesforce and Microsoft Corporation and believe that Social Solutions Global, Inc. provides the best data management system for the cost because no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

ACTION REQUESTED OF THE CITY COUNCIL

Adopt A Resolution:

(1) Authorizing The City Administrator To Waive the Local and Small Local Business Enterprise Program (L/SLBE) and the Competitive Bidding Process and Award a Five-Year Contract, From August 1, 2022 To June 30, 2027, To Social Solutions Global, Inc. For The Development Of An Apricot 360 Data Management System and For Annual Licensing And Technical Assistance Fees For a Total Amount Not To Exceed Five Hundred Thirty-Three Thousand Fifty-Six Dollars ($533,056); And (2) Adopting The Surveillance Use Policy Attached Hereto As Exhibit A Pertaining To The Apricot 360 Data Management System.

For questions regarding this report, please contact Guillermo Cespedes at 510-238-2916.

Respectfully submitted,

_____
Guillermo Cespedes (Jul 6, 2022 17:20 PDT)
_____

GUILLERMO CESPEDES
Chief, Department of Violence Prevention

Reviewed by:
Mailee Wang, Administrative Services Manager

Prepared by:
Jenny Linchey, Budget and Grants
Administrator

Attachments (2):
A: Apricot 360 Surveillance Use Policy – Version A
B: Apricot 360 Surveillance Use Policy – Version B
Exhibit A to Resolution Apricot 360 Surveillance Use Policy – Version A

Apricot 360 Use Policy – VERSION A
City of Oakland Department of Violence Prevention

The Department of Violence Prevention (DVP) formed in 2020 with a mandate to reduce levels of gun violence, intimate partner violence, commercial sexual exploitation, family trauma associated with unsolved homicides, and community trauma associated with ongoing violence in Oakland. The DVP applies a public health approach to violence prevention and intervention efforts that focuses resources on people, neighborhoods, and times of day that are most likely to be impacted by violence. The department also applies different prevention and intervention strategies based on whether individuals are exposed to violence, at risk for violence, or at the center of violence. Each fiscal year, the DVP distributes millions of dollars in funding to community-based organizations (CBOs) in Oakland that deliver prevention and intervention services in the areas of group and gun violence, gender-based violence, and community healing. The DVP also provides direct services in the areas of adult life coaching, violence interruption, and shooting and homicide response.

A. Purpose

The Apricot 360 data management system (Apricot 360), developed by Bonterra (formerly Social Solutions Global, Inc.), will enable the DVP and its contracted CBOs to track information related to service delivery and contract management in the DVP's three strategy areas of group and gun violence, gender-based violence, and community healing. Apricot 360 will be used by direct service staff within the DVP and CBOs to track client enrollment, service engagement, milestones, and outcomes for individual services as well as attendance, duration, and content of group services. Supervisory staff within the DVP and CBOs will use the system to ensure that direct service staff are engaging clients with the expected frequency and delivering services appropriately to facilitate behavior change. The DVP's data and evaluation staff will use Apricot 360 to monitor service delivery and outcome data across each strategy, oversee the activities and deliverables of individual CBOs to ensure alignment with scopes of work and service models, and identify challenges with service delivery that require remediation. Fiscal and contract staff within the DVP and CBOs will use the system to store contract documents, communicate about contract questions, track budget spenddown, and process invoices based on completion of deliverables. Finally, service delivery and outcome data collected through Apricot 360 will be available to external evaluators contracted by the City of Oakland to conduct an evaluation of DVP programs and services.

B. Authorized Use

Data stored in Apricot 360 will be accessed on a need-to-know and right-to-know basis, meaning that DVP and CBO staff members will only have to access information that is essential to their job function. Categories of Apricot 360 system usage are described below.

- **Service delivery:** Direct service and supervision staff employed by the DVP and contracted CBOs will use Apricot 360 to track information on client enrollment, contacts, progress towards milestones, accomplishments, referrals, and other aspects of service delivery. The system will identify upcoming staff member tasks related to service delivery and present summarized data on clients served though dashboards that are helpful to staff. Direct service staff include individuals such as case managers and life coaches who work directly with clients to deliver services or programming. Supervision staff are supervisors of direct service staff.

- **Violent incident crisis response coordination:** Violence interrupters employed through the DVP and contracted CBOs will receive information about shootings and homicides through Apricot 360 and enter information pertaining to their response. Select staff members within the DVP who coordinate the 24/7 response to shootings and homicides will review data entered by contracted CBOs pertaining to shooting and homicide response activities to ensure that victims and family members receive timely, comprehensive, and coordinated support services. These staff members will also use Apricot 360 to monitor and coordinate violence interruption activities to prevent retaliation.

- **Program monitoring and accountability:** DVP data and evaluation staff will use aggregate service delivery data to monitor trends in service delivery within activities and substrategies and ensure that summarized service delivery data are available to a range of external stakeholders, including councilmembers, committee members, grantors, and the public. DVP data and evaluation staff will also review individual-level client data within the group and gun violence strategy to determine how many clients are enrolled in multiple services, ensure that clients are not simultaneously enrolled in the same service through different providers, and ensure that services delivered to individual clients meet DVP expectations in terms of quality, frequency, duration, and reach.

- **Contract management:** Fiscal and contract staff employed by the DVP and contracted CBOs will use the system to manage grant budgets, monitor contract deliverables, process budget modifications and payments, and communicate about contracts.

- **External evaluation:** External evaluators contracted by the City of Oakland will use data from Apricot 360 to evaluate the effectiveness of services delivered by the DVP and contracted CBOs. Evaluators will seek and receive institutional review board (IRB) approval prior to commencing research activities. Once IRB approval is obtained, evaluators will only have access to personally-identifiable information for individuals who have signed a consent form agreeing to have their identifiable data shared with a third-party evaluator. For clients who do not sign a consent form, evaluators will receive deidentified or aggregate data.

C. Data Collection

Service delivery data will be entered into Apricot 360 by direct service staff employed by the DVP and contracted CBOs. For each activity funded through the DVP's three strategies, **Tables 1-3** identify which data entry forms will be completed. **Table 4** provides an overview of the types of data collected through each form.

Table 1. Data entry forms completed in Apricot 360 for the DVP's group and gun violence strategy.

Substrategy	Activity	Client record	Family support	Group activity	Hospital response	Life map goals and activities	Non-program service delivery	Program enrollment & exit	Program intake & needs assessment	Program service delivery	Referral to services	Relocation	Triangle incident response	Violence mediation
Employment & Education Support Services	Adult employment & education services	x		x				x		x	x			
	Youth job exploration & education services	x		x				x		x	x			
School Site Violence Intervention & Prevention Teams	Community healing			x										
	Gender-based violence: Individual-level services						x				x			
	Gender-based violence: Group services			x										
	Violence interruption										x			x
	Youth life coaching	x				x		x	x	x	x			
Violent incident crisis response	Emergency relocation											x		
	Family support following homicide		x								x			
	Hospital intervention				x						x			
	Violence interruption										x		x	x
Youth Diversion and Youth & Adult Life Coaching	Adult life coaching	x				x		x	x	x	x			
	Housing-focused case management	x						x	x	x	x			
	Youth diversion: Individual-level services						x							x
	Youth diversion: Group-level services			x										
	Youth life coaching	x				x		x	x	x	x			

Table 2. Data entry forms completed in Apricot 360 for the DVP's gender-based violence strategy.

Substrategy	Activity	Client record	Drop-in center	GBV crisis line	Group activity	Life map goals and activities	Mobile advocacy	Non-program service delivery	Program enrollment & exit	Program intake & needs assessment	Program service delivery	Referral to services	Relocation	Triangle incident response
Crisis response	Bedside advocacy and accompaniment						x					x		
	24-hour hotlines			x										
Housing	Emergency shelter: Hotel vouchers							x						

Substrategy	Activity	Forms completed in Apricot 360 database												
		Client record	Drop-in center	GBV crisis line	Group activity	Life map goals and activities	Mobile advocacy	Non-program service delivery	Program enrollment & exit	Program intake & needs assessment	Program service delivery	Referral to services	Relocation	Triangle incident response
	Emergency shelter: Relocation												x	
	Transitional housing							x				x		
Wrap-Around Services	Employment support: Individual services	x							x		x			
	Employment support: Group services				x									
	Legal advocacy: Advice and referral							x				x		
	Legal advocacy: Case management	x							x		x			
	Life coaching	x				x			x	x	x	x		
	Safe space alternatives		x		x							x		
	Therapeutic support: Individual services	x							x		x			
	Therapeutic support: Group services				x									

Table 3. Data entry forms completed in Apricot 360 for the DVP's community healing strategy.

Substrategy	Forms completed in Apricot 360 database							
	Client record	Family support	Group activity	Mini grant	Outreach	Program enrollment & exit	Program service delivery	Referral to services
Restorative services			x					
Mini grants				x				
Neighborhood and community teams					x			x
Therapeutic supports: Individual-level services	x					x	x	
Therapeutic supports: Group-level services			x					
Town Nights			x					

Table 4. Types of data collected through Apricot 360 forms.

Form	Data fields
Client record	1. Name and date of birth[*] 2. Contact information[*] 3. Demographic information (race, gender, education, language spoken at home) 4. Employment status 5. Housing status 6. School information, if applicable

Form	Data fields
	7. Names and contact information of important people, if client chooses to provide (e.g. probation officer)
Drop-in center	1. Date of visit 2. Basic demographics (age, gender, race)
Family support	1. Name of homicide victim 2. Number of individuals in family 3. Types and amount of support provided (e.g. relocation, funeral/vigil planning, VOC applications, financial) 4. Attendance at funerals/vigils
GBV crisis line	1. Time and date of call 2. Yes/No: Did call relate to GBV? 3. Basic demographic information (age, race, gender)
Group activity	1. Date, location, and duration of activity 2. Number and type (e.g. students, residents, teachers) of people in attendance 3. Type of activity (e.g. training, support group)
Mobile/bedside advocacy	1. Date and time of contact 2. Basic demographic information (age, gender, race) 3. Yes/No: Was safety plan developed?
Hospital response	1. Date and time of initial notification 2. Date and time of visits for service 3. Name and date of birth of individual visited 4. Type of support provided (e.g. VOC applications, relocation funding)
Life map goals and activities	1. Case plan goals 2. Planned and accomplished actions associated with goals 3. Start dates, completion dates, and current progress 4. Date and amount of financial incentives provided for completion of life map goals
Mini grant	1. Grant amount, term, and recipient 2. Activities planned with grant 3. Number of people served through grant
Non-program service delivery	1. Name and date of birth[*] 2. Basic demographic information (age, gender, race) 3. Date of service provided 4. Type of service provided (e.g. housing, legal services) 5. Length of service, if applicable (e.g. length of stay in temporary housing)
Outreach	1. Name and contact information 2. Basic demographic information (age, gender, race) 3. Date, method, and outcome of all outreach attempts 4. Referral source
Program enrollment & exit	1. Date and source of referral 2. Dates of enrollment and exit 3. Type of program 4. Reason for exit
Program intake and needs assessment	1. Date of intake and needs assessment 2. Other questions will be specific to strategy or service provider
Program service delivery	1. Date, duration, method, and outcome of communication with client by service provider 2. Date and amount of financial incentives provided to client 3. Assigned staff member's name
Referral to services	1. Name and date of birth[*] 2. Date of referral 3. Type of service referral

Form	Data fields
	4. Name of organization referred to
	5. Status of referral (e.g. sent, received, accepted, denied)
Relocation	1. Names of individuals being relocated
	2. Yes/No: Was safety assessment conducted?
	3. Date and types of relocation support provided
	4. Date and result of request for relocation support/funding
Triangle incident response	1. Date and time of notification
	2. Date and time of scene or hospital response
	3. Assessment: Victim name and demographics, category of incident, homicide (yes/no), level of retaliation
	4. Notes on follow-up: relocation, mediation, peer outreach, family outreach, school outreach, community outreach
Violence mediation	1. Date and time of mediation conversations
	2. Names of individuals involved in conversations
	3. Type of mediation: proactive vs. retaliation
	4. Other people notified of conflict (e.g. family members, school administrators)

*These fields are applicable for activities that require entry of personally-identifiable information.

For each strategy and activity, **Tables 5-7** identify whether CBOs will be expected to enter individual-level client records and personally-identifiable information (PII). For this use policy, PII refers to an individual's full name and may also include the individual's date of birth. In situations where individual client records are required but PII is not, agencies will be able to leave the first and last name fields blank. **Tables 5-7** also identify whether select DVP staff (described under *Data Access*) will be able to view individual-level client records and PII for purposes of data quality assurance, process evaluation, and service coordination.

Table 5. Entry and visibility of individual-level client records and PII for the DVP's group and gun violence strategy.

Substrategy	Activity	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
Employment & Education Support Services	Adult employment & education services	Yes	Yes	Yes
	Youth job exploration & education services	Yes	Yes	Yes
School Site Violence Intervention & Prevention Teams	Community healing	No	No	No
	Gender-based violence: Individual-level services	Yes	Provider choice	No
	Gender-based violence: Group services	No	No	No
	Violence interruption	Yes	Yes	Yes
	Youth life coaching	Yes	Yes	Yes
Violent incident crisis response	Emergency relocation	Yes	Yes	Yes
	Family support following homicide	Yes	Yes	Yes
	Hospital intervention	Yes	Yes	Yes
	Violence interruption	Yes	Yes	Yes
Youth Diversion and Youth & Adult Life Coaching	Adult life coaching	Yes	Yes	Yes
	Housing-focused case management	Yes	Yes	Yes
	Youth diversion: Individual-level services	Yes	Yes	Yes

Substrategy	Activity	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
	Youth diversion: Group-level services	No	No	No
	Youth life coaching	Yes	Yes	Yes

Table 6. Entry and visibility of individual-level client records and PII for the DVP's gender-based violence strategy.

Substrategy	Activity	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
Crisis response	Bedside advocacy and accompaniment	Yes	Provider choice	No
	24-hour hotlines	Provider choice	Provider choice	No
Housing	Emergency shelter: Hotel vouchers	Provider choice	Provider choice	No
	Emergency shelter: Relocation	Yes	Provider choice	No
	Transitional housing	Yes	Provider choice	No
Wrap-Around Services	Employment support: Individual services	Yes	Provider choice	No
	Employment support: Group services	No	No	No
	Legal advocacy: Advice and referral	Provider choice	Provider choice	No
	Legal advocacy: Case management	Yes	Provider choice	No
	Life coaching	Yes	Provider choice	No
	Safe space alternatives	Provider choice	Provider choice	No
	Therapeutic support: Individual services	Yes	Provider choice	No
	Therapeutic support: Group services	No	No	No

Table 7. Entry and visibility of individual-level client records and PII for the DVP's community healing strategy.

Substrategy	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
Restorative services	No	No	No
Mini grants	No	No	No
Neighborhood and community teams	Yes	Yes	No
Therapeutic supports: Individual-level services	Yes	Yes	No
Therapeutic supports: Group-level services	No	No	No
Town Nights	No	No	No

For activities that collect PII, regardless of visibility to DVP staff, CBOs will be encouraged to notify clients that their name and date of birth will be documented in Apricot 360 for purposes of effective service delivery and coordination. Clients will also be asked to sign a consent form regarding potential access to their PII by a third-party evaluator. Completion of this consent form is strongly encouraged but is not a requirement of service delivery for any strategy, and clients will be able to decline having their PII accessed by a third-party evaluator if they wish.

D. Data Access

The DVP will take special care to ensure that data within Apricot 360 are accessed on a need-to-know and right-to-know basis, meaning that staff will only be able to access information that is essential to their job function. Apricot 360 allows administrators to restrict access to individual forms, records, and fields for staff members based on their pre-determined access requirements. An overview of data access levels for categories of staff employed by the DVP and contracted CBOs is provided below:

Contracted CBOs

- *Direct service staff and supervisors* will have access to individual- and group-level service delivery data entered by members of their agency only. Direct service staff and supervisors will NOT have access to service-delivery data for clients being served by other agencies, even if they are the same clients.

- *Fiscal and contract staff* will have access to contract and fiscal documents such as budgets, scopes of work, invoices, and payments for their agency only. These staff members will also have access to aggregate service delivery data pertaining to contract deliverables, which will be automatically calculated based on data entered by direct service staff. Fiscal and contract staff will not have access to individual client records or PII.

DVP

- *Direct service staff and supervisors* will have access to individual- and group-level service delivery data entered by members of the DVP only. Direct service staff and supervisors within the DVP will NOT have access to service-delivery data for clients being served by other agencies, even if they are the same clients.

- *Violent incident crisis response coordination staff* will have access to data entered by staff within the DVP and contracted CBOs pertaining to the violence incident crisis response substrategy to ensure timely coordination of support services and violence interruption activities to prevent retaliation. This will include access to names of individuals involved in violent incident crisis response activities and services.

- *Fiscal and contract staff* will have access to contract and fiscal documents such as budgets, scopes of work, invoices, and payments for all grantees. These staff members will also have access to aggregate service delivery data pertaining to contract deliverables, which will be automatically calculated based on data entered by direct service staff. Fiscal and contract staff will not have access to individual client records or PII.

- **Data and evaluation staff within the DVP** will have access to client-level data and PII for DVP clients across all substrategies. For clients engaged by contracted CBOs, DVP data and evaluation staff will also have access to client-level data and PII for activities within the group and gun violence strategy for the purpose of identifying and remediating issues related to service delivery within or across CBOs.

- **External data and evaluation staff** employed by evaluation firms contracted by the City of Oakland will have access to PII for clients who have previously consented to having their PII shared with an external evaluator. For clients who have not consented to having their PII shared, external evaluation firms will only receive access to deidentified or aggregate service delivery data. All data shared with external evaluators will be downloaded from Apricot 360 by Bonterra technical support staff and shared via a secure file transfer method.

Unauthorized use of the system by any staff person with any level of access will lead to disciplinary action, which could include the termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

E. Data Protection

Apricot 360 has comprehensive measures in place to maintain data privacy and security. The system sits behind a firewall that extensively controls, tracks, and reports access to the system's internal infrastructure. Apricot 360 meets current U.S. Department of Housing and Urban Development (HUD) domestic violence standards, Homeless Management Information System (HMIS) standards, and Social Security Administration data management and security protocols, as well as minimum required Family Educational Rights and Privacy Act (FERPA) and HIPAA standards. Data entered into Apricot 360 are automatically encrypted while in transit between a user's computer and the system's servers, as well as while at rest. Additionally, users accessing Apricot 360 servers do so via a secure HTTPS connection. More information on privacy and security for the Apricot 360 system is included in **Attachment A.**

F. Data Retention

Agencies that collect PII for clients based on their funded activities will be required to retain the PII for three years following service completion to ensure that data are available for evaluations conducted by external evaluators, which can last for up to three years following service delivery. At the end of three years, agencies will delete PII unless exempted based on legal requirements. Anonymous service delivery data will be retained for an additional four years to allow the DVP to monitor trends in service delivery over time. At the conclusion of seven years, individual-level data will be permanently deleted from Apricot 360 unless exempted due to legal requirements.

G. Public Access

There will be absolutely no public access to individual-level client data in Apricot 360. As with any government record, a member of the public may submit a Public Records Act request, but only aggregate data (no PII) would be released subject to applicable federal, state, and local privacy or confidentiality laws. If the DVP receives a request of this nature, staff will work with the City Attorney's Office to respond to the request without sharing PII. The DVP will also notify any contracted CBOs impacted by the data request as soon as reasonably possible. To date, the City of Oakland has only

received requests through the Public Records Act for aggregate-level data pertaining to its violence prevention and intervention services (e.g. how many participants were served in a year). Aggregate data from Apricot 360 will be available in evaluation reports published by third-party evaluation firms and may be shared through public tables, charts, or dashboards created by the DVP.

H. Third Party Data Sharing

Outside of the DVP, DVP-funded CBOs, and evaluation firms contracted by the City of Oakland, no other agency will have access to data collected in Apricot 360. External evaluators contracted by the City of Oakland will use data in Apricot 360 to evaluate the effectiveness of funded programs. External evaluators will only have access to PII for individuals who sign a consent form allowing their PII to be shared with a third-party evaluator. For clients who do not sign a consent form allowing access to their PII, external evaluators will receive deidentified or aggregate data.

I. Training

The DVP's data and evaluation staff will attend Apricot 360 train-the-trainer and custom end user training sessions, which will review Apricot 360's configuration and tips and tricks for training end users. In addition, DVP staff will have access to the Apricot basic training package, which includes unlimited access to the following:

- Live Apricot setup webinar
- Live Apricot insights webinar
- Administrative video library
- End user training library

Using these tools, the DVP's data and evaluation staff will train direct service staff, supervisors, and contract and fiscal staff within the DVP and contracted CBOs on how to use Apricot 360. This will include general trainings, trainings specific to substrategies and activities, and ongoing options for one-on-one training, support, and technical assistance. All trainings will specify appropriate usage of the system pertaining to data privacy and security as outlined in this use policy, and all trained staff members will sign a copy of the use policy indicating that they have read and understand it. Trainings will also discuss consequences of inappropriate system usage, which could include termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

Additionally, all staff within the DVP who have access to client-level data and PII entered into Apricot 360 by contracted CBOs will maintain current certifications in HIPAA and Collaborative Institutional Training Initiative (CITI) research, ethics, and compliance training.

J. Auditing and Oversight

The DVP's data and evaluation staff will monitor compliance with this use policy of staff within the DVP and contracted CBOs. All actions in the system (add, edit, delete, view, etc.) are accessible through audit log reports built into the system for administrator monitoring. On a quarterly basis, the DVP's data and evaluation staff will receive these logs from Apricot 360 administrators and review them for any signs of inappropriate system usage. Any indication of inappropriate system usage will be thoroughly investigated by the DVP in consultation with the City Attorney's Office. Inappropriate system usage

could result in termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

K. Maintenance

Bonterra's security mechanisms and procedures are built on the Soc2 Type II Framework with HIPAA amendment and audited by third-party security experts annually to ensure compliance with best-in-class technical safeguards, processes, policies, and procedures. Bonterra has an extensive cloud security team led by their Chief Information Security Officer that uses a broad set of tools for monitoring security, vulnerability, integrity, and uptime across over 19,000 customers. A complete copy of Bonterra.'s Soc2 Type II has been shared with City of Oakland staff who have signed a non-disclosure agreement, including data and evaluation staff from the DVP and staff from the Information Technology Department.

Social Solutions Global, Inc. ("SSG") takes comprehensive measures to attempt to ensure that data is kept safe, confidential and recoverable in the case of a disaster. Social Solutions' office sits behind a firewall which extensively controls, tracks, and reports access to our internal infrastructure. Our software meets current required HIPAA standards.

Data Security

Apricot® uses user names and passwords to prevent unauthorized access and to restrict user access within the application. Each unique user account is assigned access to programs and permission sets to restrict access to data and features in the system. Customer data is housed in two locations (U.S. and Canada) based on the location of the client. Data is stored using redundant AWS hardware technologies and SSG fault tolerant software and journaling file systems.

Passwords

✓ can be set to have a minimum length

✓ can be set to contain non-alpha-numeric characters

✓ can be set to expire

✓ can be locked after a set # of invalid login attempts

✓ can be changed by a local administrator

✓ are not displayed upon entry and are encrypted

Encryption

Social Solutions uses state-of-the-art equipment and technology to safeguard the confidential nature of your data. Your data is automatically encrypted while in transit between your computer and our servers as well as while in the database. Social Solutions uses the largest commercially available SSL cipher key size of 2048 bits. Users access Apricot® software web application servers via secure HTTPS connection.

SOC2

Our SOC2 Type 2 (SSAE18) report is a comprehensive document that describes Social Solutions security controls in the domains of Administrative, Physical, and Technical security. Apricot is certified SOC 2 Type II compliant. SSG security controls are reviewed by independent external auditors during audits for our SOC compliance.

Amazon Web Services (AWS) Server Security

Each of our servers is individually governed by a system that is designed to prevent unexpected Internet data from being processed by our server software. IDS, virus scanning, automated system checks, and remote logging guard against unauthorized access. AWS implements electronic surveillance and multi-factor access control systems to secure its data centers. Data centers are staffed 24x7 by trained security guards, and access must be strictly authorized. Multiple availability zones allow Apricot® to remain resilient in the face of most failure modes, including natural disasters or system failures[1]. In case of a disaster in our main AWS region, Social Solutions will have Apricot® up and running between 24-48 hours in a backup AWS region.

Redundant Infrastructure and Backups

✓ 24/7/365 monitoring of uptime across the infrastructure

✓ Redundant water, power, telecommunications, and internet connectivity to maintain continuous operations

✓ Uninterrupted power supply to reduce possible service outages

Retention Policy

Keep daily backups for 12 months

Compliance

The AWS cloud infrastructure has been designed and managed by Amazon.com[2]. AWS adheres to:
SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)   SOC 2   SOC 3   PCI DSS Level 1 ISO 270012

1 For additional information visit: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

2 For additional information visit: https://d0.awsstatic.com/whitepapers/compliance/AWS_Compliance_Quick_Reference.pdf

Apricot 360 Use Policy – VERSION B
City of Oakland Department of Violence Prevention

The Department of Violence Prevention (DVP) formed in 2020 with a mandate to reduce levels of gun violence, intimate partner violence, commercial sexual exploitation, family trauma associated with unsolved homicides, and community trauma associated with ongoing violence in Oakland. The DVP applies a public health approach to violence prevention and intervention efforts that focuses resources on people, neighborhoods, and times of day that are most likely to be impacted by violence. The department also applies different prevention and intervention strategies based on whether individuals are exposed to violence, at risk for violence, or at the center of violence. Each fiscal year, the DVP distributes millions of dollars in funding to community-based organizations (CBOs) in Oakland that deliver prevention and intervention services in the areas of group and gun violence, gender-based violence, and community healing. The DVP also provides direct services in the areas of adult life coaching, violence interruption, and shooting and homicide response.

A. Purpose

The Apricot 360 data management system (Apricot 360), developed by Bonterra (formerly Social Solutions Global, Inc.), will enable the DVP and its contracted CBOs to track information related to service delivery and contract management in the DVP's three strategy areas of group and gun violence, gender-based violence, and community healing. Apricot 360 will be used by direct service staff within the DVP and CBOs to track client enrollment, service engagement, milestones, and outcomes for individual services as well as attendance, duration, and content of group services. Supervisory staff within the DVP and CBOs will use the system to ensure that direct service staff are engaging clients with the expected frequency and delivering services appropriately to facilitate behavior change. The DVP's data and evaluation staff will use Apricot 360 to monitor service delivery and outcome data across each strategy, oversee the activities and deliverables of individual CBOs to ensure alignment with scopes of work and service models, and identify challenges with service delivery that require remediation. Fiscal and contract staff within the DVP and CBOs will use the system to store contract documents, communicate about contract questions, track budget spenddown, and process invoices based on completion of deliverables. Finally, service delivery and outcome data collected through Apricot 360 will be available to external evaluators contracted by the City of Oakland to conduct an evaluation of DVP programs and services.

B. Authorized Use

Data stored in Apricot 360 will be accessed on a need-to-know and right-to-know basis, meaning that DVP and CBO staff members will only have to access information that is essential to their job function. Categories of Apricot 360 system usage are described below.

- **Service delivery:** Direct service and supervision staff employed by the DVP and contracted CBOs will use Apricot 360 to track information on client enrollment, contacts, progress towards milestones, accomplishments, referrals, and other aspects of service delivery. The system will identify upcoming staff member tasks related to service delivery and present summarized data on clients served though dashboards that are helpful to staff. Direct service staff include individuals such as case managers and life coaches who work directly with clients to deliver services or programming. Supervision staff are supervisors of direct service staff.

- **Program monitoring and accountability:** DVP data and evaluation staff will use aggregate service delivery data to monitor trends in service delivery within activities and substrategies and ensure that summarized service delivery data are available to a range of external stakeholders, including councilmembers, committee members, grantors, and the public

- **Contract management:** Fiscal and contract staff employed by the DVP and contracted CBOs will use the system to manage grant budgets, monitor contract deliverables, process budget modifications and payments, and communicate about contracts.

- **External evaluation:** External evaluators contracted by the City of Oakland will use data from Apricot 360 to evaluate the effectiveness of services delivered by the DVP and contracted CBOs. Evaluators will seek and receive institutional review board (IRB) approval prior to commencing research activities. Once IRB approval is obtained, evaluators will only have access to personally-identifiable information for individuals who have signed a consent form agreeing to have their identifiable data shared with a third-party evaluator. For clients who do not sign a consent form, evaluators will receive deidentified or aggregate data.

C. Data Collection

Service delivery data will be entered into Apricot 360 by direct service staff employed by the DVP and contracted CBOs. For each activity funded through the DVP's three strategies, **Tables 1-3** identify which data entry forms will be completed. **Table 4** provides an overview of the types of data collected through each form.

Table 1. Data entry forms completed in Apricot 360 for the DVP's group and gun violence strategy.

Substrategy	Activity	Client record	Family support	Group activity	Hospital response	Life map goals and activities	Non-program service delivery	Program enrollment & exit	Program intake & needs assessment	Program service delivery	Referral to services	Relocation	Triangle incident response	Violence mediation
Employment & Education Support Services	Adult employment & education services	x		x				x		x	x			
	Youth job exploration & education services	x		x				x		x	x			
School Site Violence Intervention & Prevention Teams	Community healing			x										
	Gender-based violence: Individual-level services						x				x			
	Gender-based violence: Group services			x										
	Violence interruption										x			x
	Youth life coaching	x				x		x	x	x	x			
Violent incident crisis response	Emergency relocation											x		
	Family support following homicide		x								x			
	Hospital intervention				x						x			
	Violence interruption										x		x	x

Substrategy	Activity	Forms completed in Apricot 360 database												
		Client record	Family support	Group activity	Hospital response	Life map goals and activities	Non-program service delivery	Program enrollment & exit	Program intake & needs assessment	Program service delivery	Referral to services	Relocation	Triangle incident response	Violence mediation
Youth Diversion and Youth & Adult Life Coaching	Adult life coaching	x				x		x	x	x	x			
	Housing-focused case management	x						x		x	x			
	Youth diversion: Individual-level services						x							x
	Youth diversion: Group-level services			x										
	Youth life coaching	x				x		x	x	x	x			

Table 2. Data entry forms completed in Apricot 360 for the DVP's gender-based violence strategy.

Substrategy	Activity	Forms completed in Apricot 360 database												
		Client record	Drop-in center	GBV crisis line	Group activity	Life map goals and activities	Mobile advocacy	Non-program service delivery	Program enrollment & exit	Program intake & needs assessment	Program service delivery	Referral to services	Relocation	Triangle incident response
Crisis response	Bedside advocacy and accompaniment						x					x		
	24-hour hotlines			x										
Housing	Emergency shelter: Hotel vouchers							x						
	Emergency shelter: Relocation												x	
	Transitional housing							x				x		
Wrap-Around Services	Employment support: Individual services	x							x		x			
	Employment support: Group services				x									
	Legal advocacy: Advice and referral							x				x		
	Legal advocacy: Case management	x							x		x			
	Life coaching	x					x		x	x	x	x		
	Safe space alternatives		x		x							x		
	Therapeutic support: Individual services	x							x		x			
	Therapeutic support: Group services				x									

Table 3. Data entry forms completed in Apricot 360 for the DVP's community healing strategy.

Substrategy	Forms completed in Apricot 360 database							
	Client record	Family support	Group activity	Mini grant	Outreach	Program enrollment & exit	Program service delivery	Referral to services
Restorative services			x					
Mini grants				x				
Neighborhood and community teams					x			x
Therapeutic supports: Individual-level services	x					x	x	
Therapeutic supports: Group-level services			x					
Town Nights			x					

Table 4. Types of data collected through Apricot 360 forms.

Form	Data fields
Client record	1. Name and date of birth[*] 2. Contact information[*] 3. Demographic information (race, gender, education, language spoken at home) 4. Employment status 5. Housing status 6. School information, if applicable 7. Names and contact information of important people, if client chooses to provide (e.g. probation officer)
Drop-in center	1. Date of visit 2. Basic demographics (age, gender, race)
Family support	1. Name of homicide victim 2. Number of individuals in family 3. Types and amount of support provided (e.g. relocation, funeral/vigil planning, VOC applications, financial) 4. Attendance at funerals/vigils
GBV crisis line	1. Time and date of call 2. Yes/No: Did call relate to GBV? 3. Basic demographic information (age, race, gender)
Group activity	1. Date, location, and duration of activity 2. Number and type (e.g. students, residents, teachers) of people in attendance 3. Type of activity (e.g. training, support group)
Mobile advocacy	1. Date and time of contact 2. Basic demographic information (age, gender, race) 3. Yes/No: Was safety plan developed?
Hospital response	1. Date and time of initial notification 2. Date and time of visits for service 3. Name and date of birth of individual visited 4. Type of support provided (e.g. VOC applications, relocation funding)
Life map goals and activities	1. Case plan goals 2. Planned and accomplished actions associated with goals 3. Start dates, completion dates, and current progress 4. Date and amount of financial incentives provided for completion of life map goals
Mini grant	1. Grant amount, term, and recipient 2. Activities planned with grant 3. Number of people served through grant

Form	Data fields
Non-program service delivery	1. Name and date of birth* 2. Basic demographic information (age, gender, race) 3. Date of service provided 4. Type of service provided (e.g. housing, legal services) 5. Length of service, if applicable (e.g. length of stay in temporary housing)
Outreach	1. Name and contact information 2. Basic demographic information (age, gender, race) 3. Date, method, and outcome of all outreach attempts 4. Referral source
Program enrollment & exit	1. Date and source of referral 2. Dates of enrollment and exit 3. Type of program 4. Reason for exit
Program intake and needs assessment	1. Date of intake and needs assessment 2. Other questions will be specific to strategy or service provider
Program service delivery	1. Date, duration, method, and outcome of communication with client by service provider 2. Date and amount of financial incentives provided to client 3. Assigned staff member's name
Referral to services	1. Name and date of birth* 2. Date of referral 3. Type of service referral 4. Name of organization referred to 5. Status of referral (e.g. sent, received, accepted, denied)
Relocation	1. Names of individuals being relocated 2. Yes/No: Was safety assessment conducted? 3. Date and types of relocation support provided 4. Date and result of request for relocation support/funding
Triangle incident response	1. Date and time of notification 2. Date and time of scene or hospital response 3. Assessment: Victim name and demographics, category of incident, homicide (yes/no), level of retaliation 4. Notes on follow-up: relocation, mediation, peer outreach, family outreach, school outreach, community outreach
Violence mediation	1. Date and time of mediation conversations 2. Names of individuals involved in conversations 3. Type of mediation: proactive vs. retaliation 4. Other people notified of conflict (e.g. family members, school administrators)

*These fields are applicable for activities that require entry of personally-identifiable information.

For each strategy and activity, **Tables 5-7** identify whether CBOs will be expected to enter individual-level client records and personally-identifiable information (PII). For this use policy, PII refers to an individual's full name and may also include the individual's date of birth. In situations where individual client records are required but PII is not, agencies will be able to leave the first and last name fields blank. **Tables 5-7** also indicate that individual-level records and PII entered by CBOs will not be visible to DVP; DVP staff will only have access to aggregate service-delivery data entered by CBOs across all strategies.

Table 5. Entry and visibility of individual-level client records and PII for the DVP's group and gun violence strategy.

Substrategy	Activity	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
Employment & Education Support Services	Adult employment & education services	Yes	Yes	No
	Youth job exploration & education services	Yes	Yes	No
School Site Violence Intervention & Prevention Teams	Community healing	No	No	No
	Gender-based violence: Individual-level services	Yes	Provider choice	No
	Gender-based violence: Group services	No	No	No
	Violence interruption	Yes	Yes	No
	Youth life coaching	Yes	Yes	No
Violent incident crisis response	Emergency relocation	Yes	Yes	No
	Family support following homicide	Yes	Yes	No
	Hospital intervention	Yes	Yes	No
	Violence interruption	Yes	Yes	No
Youth Diversion and Youth & Adult Life Coaching	Adult life coaching	Yes	Yes	No
	Housing-focused case management	Yes	Yes	No
	Youth diversion: Individual-level services	Yes	Yes	No
	Youth diversion: Group-level services	No	No	No
	Youth life coaching	Yes	Yes	No

Table 6. Entry and visibility of individual-level client records and PII for the DVP's gender-based violence strategy.

Substrategy	Activity	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
Crisis response	Bedside advocacy and accompaniment	Yes	Provider choice	No
	24-hour hotlines	Provider choice	Provider choice	No
Housing	Emergency shelter: Hotel vouchers	Provider choice	Provider choice	No
	Emergency shelter: Relocation	Yes	Provider choice	No
	Transitional housing	Yes	Provider choice	No
Wrap-Around Services	Employment support: Individual services	Yes	Provider choice	No
	Employment support: Group services	No	No	No
	Legal advocacy: Advice and referral	Provider choice	Provider choice	No
	Legal advocacy: Case management	Yes	Provider choice	No
	Life coaching	Yes	Provider choice	No
	Safe space alternatives	Provider choice	Provider choice	No

Substrategy	Activity	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
	Therapeutic support: Individual services	Yes	Provider choice	No
	Therapeutic support: Group services	No	No	No

Table 7. Entry and visibility of individual-level client records and PII for the DVP's community healing strategy.

Substrategy	Are individual client records entered?	Is PII entered?	Are individual records and PII entered by CBOs visible to DVP staff?
Restorative services	No	No	No
Mini grants	No	No	No
Neighborhood and community teams	Yes	Yes	No
Therapeutic supports: Individual-level services	Yes	Yes	No
Therapeutic supports: Group-level services	No	No	No
Town Nights	No	No	No

For activities that collect PII, regardless of the fact that data will not be visible to DVP staff, CBOs will be encouraged to notify clients that their name and date of birth will be documented in Apricot 360 for purposes of effective service delivery and coordination. Clients will also be asked to sign a consent form regarding potential access to their PII by a third-party evaluator. Completion of this consent form is strongly encouraged but is not a requirement of service delivery for any strategy, and clients will be able to decline having their PII accessed by a third-party evaluator if they wish.

D. Data Access

The DVP will take special care to ensure that data within Apricot 360 are accessed on a need-to-know and right-to-know basis, meaning that staff will only be able to access information that is essential to their job function. Apricot 360 allows administrators to restrict access to individual forms, records, and fields for staff members based on their pre-determined access requirements. An overview of data access levels for categories of staff employed by the DVP and contracted CBOs is provided below:

Contracted CBOs

- ▪ ***Direct service staff and supervisors*** will have access to individual- and group-level service delivery data entered by members of their agency only. Direct service staff and supervisors will NOT have access to service-delivery data for clients being served by other agencies, even if they are the same clients.

- ▪ ***Fiscal and contract staff*** will have access to contract and fiscal documents such as budgets, scopes of work, invoices, and payments for their agency only. These staff members will also have access to aggregate service delivery data pertaining to contract deliverables, which will be

automatically calculated based on data entered by direct service staff. Fiscal and contract staff will not have access to individual client records or PII.

DVP

- ▪ *Direct service staff and supervisors* will have access to individual- and group-level service delivery data entered by members of the DVP only. Direct service staff and supervisors within the DVP will NOT have access to service-delivery data for clients being served by other agencies, even if they are the same clients.

- ▪ *Fiscal and contract staff* will have access to contract and fiscal documents such as budgets, scopes of work, invoices, and payments for all grantees. These staff members will also have access to aggregate service delivery data pertaining to contract deliverables, which will be automatically calculated based on data entered by direct service staff. Fiscal and contract staff will not have access to individual client records or PII.

- ▪ *Data and evaluation staff within the DVP* will have access to client-level data and PII for DVP clients across all substrategies. For clients engaged by contracted CBOs, DVP data and evaluation staff will only have access to aggregate-level service delivery data.

- ▪ *External data and evaluation staff* employed by evaluation firms contracted by the City of Oakland will have access to PII for clients who have previously consented to having their PII shared with an external evaluator. For clients who have not consented to having their PII shared, external evaluation firms will only receive access to deidentified or aggregate service delivery data. All data shared with external evaluators will be downloaded from Apricot 360 by Bonterra technical support staff and shared via a secure file transfer method.

Unauthorized use of the system by any staff person with any level of access will lead to disciplinary action, which could include the termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

E. Data Protection

Apricot 360 has comprehensive measures in place to maintain data privacy and security. The system sits behind a firewall that extensively controls, tracks, and reports access to the system's internal infrastructure. Apricot 360 meets current U.S. Department of Housing and Urban Development (HUD) domestic violence standards, Homeless Management Information System (HMIS) standards, and Social Security Administration data management and security protocols, as well as minimum required Family Educational Rights and Privacy Act (FERPA) and HIPAA standards. Data entered into Apricot 360 are automatically encrypted while in transit between a user's computer and the system's servers, as well as while at rest. Additionally, users accessing Apricot 360 servers do so via a secure HTTPS connection. More information on privacy and security for the Apricot 360 system is included in **Attachment A.**

F. Data Retention

Agencies that collect PII for clients based on their funded activities will be required to retain the PII for three years following service completion to ensure that data are available for evaluations conducted by external evaluators, which can last for up to three years following service delivery. At the end of three

years, agencies will delete PII unless exempted based on legal requirements. Anonymous service delivery data will be retained for an additional four years to allow the DVP to monitor trends in service delivery over time. At the conclusion of seven years, individual-level data will be permanently deleted from Apricot 360 unless exempted due to legal requirements.

G. Public Access

There will be absolutely no public access to individual-level client data in Apricot 360. As with any government record, a member of the public may submit a Public Records Act request, but only aggregate data (no PII) would be released subject to applicable federal, state, and local privacy or confidentiality laws. If the DVP receives a request of this nature, staff will work with the City Attorney's Office to respond to the request without sharing PII. The DVP will also notify any contracted CBOs impacted by the data request as soon as reasonably possible. To date, the City of Oakland has only received requests through the Public Records Act for aggregate-level data pertaining to its violence prevention and intervention services (e.g. how many participants were served in a year). Aggregate data from Apricot 360 will be available in evaluation reports published by third-party evaluation firms and may be shared through public tables, charts, or dashboards created by the DVP.

H. Third Party Data Sharing

Outside of the DVP, DVP-funded CBOs, and evaluation firms contracted by the City of Oakland, no other agency will have access to data collected in Apricot 360. External evaluators contracted by the City of Oakland will use data in Apricot 360 to evaluate the effectiveness of funded programs. External evaluators will only have access to PII for individuals who sign a consent form allowing their PII to be shared with a third-party evaluator. For clients who do not sign a consent form allowing access to their PII, external evaluators will receive deidentified or aggregate data.

I. Training

The DVP's data and evaluation staff will attend Apricot 360 train-the-trainer and custom end user training sessions, which will review Apricot 360's configuration and tips and tricks for training end users. In addition, DVP staff will have access to the Apricot basic training package, which includes unlimited access to the following:

- Live Apricot setup webinar
- Live Apricot insights webinar
- Administrative video library
- End user training library

Using these tools, the DVP's data and evaluation staff will train direct service staff, supervisors, and contract and fiscal staff within the DVP and contracted CBOs on how to use Apricot 360. This will include general trainings, trainings specific to substrategies and activities, and ongoing options for one-on-one training, support, and technical assistance. All trainings will specify appropriate usage of the system pertaining to data privacy and security as outlined in this use policy, and all trained staff members will sign a copy of the use policy indicating that they have read and understand it. Trainings will also discuss consequences of inappropriate system usage, which could include termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

J. Auditing and Oversight

The DVP's data and evaluation staff will monitor compliance with this use policy of staff within the DVP and contracted CBOs. All actions in the system (add, edit, delete, view, etc.) are accessible through audit log reports built into the system for administrator monitoring. On a quarterly basis, the DVP's data and evaluation staff will receive these logs from Apricot 360 administrators and review them for any signs of inappropriate system usage. Any indication of inappropriate system usage will be thoroughly investigated by the DVP in consultation with the City Attorney's Office. Inappropriate system usage could result in termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

K. Maintenance

Bonterra's security mechanisms and procedures are built on the Soc2 Type II Framework with HIPAA amendment and audited by third-party security experts annually to ensure compliance with best-in-class technical safeguards, processes, policies, and procedures. Bonterra has an extensive cloud security team led by their Chief Information Security Officer that uses a broad set of tools for monitoring security, vulnerability, integrity, and uptime across over 19,000 customers. A complete copy of Bonterra.'s Soc2 Type II has been shared with City of Oakland staff who have signed a non-disclosure agreement, including data and evaluation staff from the DVP and staff from the Information Technology Department.

Social Solutions Global, Inc. ("SSG") takes comprehensive measures to attempt to ensure that data is kept safe, confidential and recoverable in the case of a disaster. Social Solutions' office sits behind a firewall which extensively controls, tracks, and reports access to our internal infrastructure. Our software meets current required HIPAA standards.

Data Security

Apricot® uses user names and passwords to prevent unauthorized access and to restrict user access within the application. Each unique user account is assigned access to programs and permission sets to restrict access to data and features in the system. Customer data is housed in two locations (U.S. and Canada) based on the location of the client. Data is stored using redundant AWS hardware technologies and SSG fault tolerant software and journaling file systems.

Passwords

✔ can be set to have a minimum length
✔ can be set to contain non-alpha-numeric characters
✔ can be set to expire
✔ can be locked after a set # of invalid login attempts
✔ can be changed by a local administrator
✔ are not displayed upon entry and are encrypted

Encryption

Social Solutions uses state-of-the-art equipment and technology to safeguard the confidential nature of your data. Your data is automatically encrypted while in transit between your computer and our servers as well as while in the database. Social Solutions uses the largest commercially available SSL cipher key size of 2048 bits. Users access Apricot® software web application servers via secure HTTPS connection.

SOC2

Our SOC2 Type 2 (SSAE18) report is a comprehensive document that describes Social Solutions security controls in the domains of Administrative, Physical, and Technical security. Apricot is certified SOC 2 Type II compliant. SSG security controls are reviewed by independent external auditors during audits for our SOC compliance.

Amazon Web Services (AWS) Server Security

Each of our servers is individually governed by a system that is designed to prevent unexpected Internet data from being processed by our server software. IDS, virus scanning, automated system checks, and remote logging guard against unauthorized access. AWS implements electronic surveillance and multi-factor access control systems to secure its data centers. Data centers are staffed 24x7 by trained security guards, and access must be strictly authorized. Multiple availability zones allow Apricot® to remain resilient in the face of most failure modes, including natural disasters or system failures[1]. In case of a disaster in our main AWS region, Social Solutions will have Apricot® up and running between 24-48 hours in a backup AWS region.

Redundant Infrastructure and Backups

✔ 24/7/365 monitoring of uptime across the infrastructure
✔ Redundant water, power, telecommunications, and internet connectivity to maintain continuous operations
✔ Uninterrupted power supply to reduce possible service outages

Retention Policy

Keep daily backups for 12 months

Compliance

The AWS cloud infrastructure has been designed and managed by Amazon.com[2]. AWS adheres to:
SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)   SOC 2   SOC 3   PCI DSS Level 1   ISO 270012