

**AMENDMENT TO AGREEMENT  
BETWEEN THE COUNTY OF SAN MATEO AND  
NOVIGO SOLUTIONS, INC.**

THIS AMENDMENT TO THE AGREEMENT, entered into this \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_, by and between the COUNTY OF SAN MATEO, hereinafter called “County,” and Novigo Solutions, Inc., hereinafter called “Contractor”;

**W I T N E S S E T H:**

WHEREAS, pursuant to Government Code Section 31000, County may contract with independent contractors for the furnishing of such services to or for County or any Department thereof;

WHEREAS, on January 24, 2017, the parties entered into an agreement (the “Agreement”) for the development and implementation of a new quality assurance review system for the Human Services Agency’s Staff Development branch, through Resolution No. #075005, in the amount of \$478,000 and for the term of January 24, 2017 through January 23, 2020; and

WHEREAS, the parties wish to amend the Agreement to allow for expansion of the modernization of HSA’s program policy handbooks, and to extend the term through September 23, 2020, and to increase the amount by \$ 289,000 for a total amount of \$767,000.

**NOW, THEREFORE, IT IS HEREBY AGREED BY THE PARTIES HERETO AS FOLLOWS:**

1. Section A, Exhibits and Attachments, is amended to read as follows:

Exhibit A—Services

Exhibit A1—Handbook Services (**New**)

Exhibit B—Payments and Rates

Exhibit B1— Handbook Payments and Rates (**New**)

Exhibit C – Performance Monitoring

Attachment H—HIPAA Business Associate Requirements Attachment I—§ 504 Compliance

Attachment IP – Intellectual Property

Attachment P – Personally Identifiable Information Requirements for County Contractors, Subcontractors, Vendors and Agents (**New**)

2. Section C, **Payments**, is amended to read as follows:

In consideration of the services provided by Contractor in accordance with all terms,

conditions, and specifications set forth in this Agreement, Exhibit A, County shall make payments to Contractor based on the rates and in the manner specified in Exhibit B. County reserves the right to withhold payment if County determines that the quantity or quality of the work performed is unacceptable. In no event shall County's total fiscal obligation under this Agreement exceed **SEVEN HUNDRED AND SIXTY SEVEN THOUSAND DOLLARS** (\$767,000)

3. Section D, **Term**, is amended to read as follows:

Subject to compliance with all terms and conditions, the term of this Agreement shall be from January 24, 2017 through September 30, 2020.

4. Paragraph T - **Compliance with Living Wage** is hereby added to the Agreement as follows:

As required by Chapter 2.88 of the San Mateo County Ordinance Code, Contractor certifies all contractor(s) and subcontractor(s) obligated under this contract shall fully comply with the provisions of the County of San Mateo Living Wage Ordinance, including, but not limited to, paying all Covered Employees the current Living Wage and providing notice to all Covered Employees and Subcontractors as required under the Ordinance.

5. Section Q, **Notices**, is amended to add the following contact:

In the case of County, to:

(For Handbooks)

Name/Title: Desi A. Tafoya, Human Services Manager, Human Services Agency

Address: 1 Davis Dr., Belmont, CA 94002

Telephone: 650-802-7974

Email: DTafoya@smcgov.org

6. **Exhibit A1**—Handbook Services is added to the Agreement and attached hereto.
7. **Exhibit B1**—Handbook Payments and Rates, is added to the Agreement and attached hereto.
8. **Attachment P**—Personally Identifiable Information Requirements for County Contractors, Subcontractors, Vendors and Agents, is added to the Agreement and attached hereto.

**All other terms and conditions of the Agreement dated January 24, 2017 between County and Contractor shall remain in full force and effect.**

In witness of and in agreement with this Agreement's terms, the parties, by their duly authorized representatives, affix their respective signatures:

For Contractor: Novigo Solutions, Inc.

Contractor Signature 

05 January 2018  
Date

Mohammed Jarood Musthafa  
Contractor Name (please print)

---

COUNTY OF SAN MATEO

By: \_\_\_\_\_  
President, Board of Supervisors, San Mateo County

Date: \_\_\_\_\_

ATTEST: \_\_\_\_\_

By: \_\_\_\_\_  
Clerk of Said Board

## **Exhibit A1 (Handbook)**

### **Services**

In consideration of the payments set forth in Exhibits B and B1, Contractor shall provide the following services:

#### **A. Program Components**

In order to improve the quality of service delivery, Contractor will provide a web-centric and easy-to-use tool that facilitates a user-centric handbook technology that can provide County Staff with accurate and rapid search results. Contractor shall provide the following:

##### **1. Handbook Features**

- Ability to search one program handbook, two program handbooks or any number of selected handbooks simultaneously
- Creation of customizable lockable handbook templates for each identified document type used in our program resource handbooks that incorporates best practice elements for ease of reading technical information
- Ability to automatically create and identify dates of revisions or newly published information for the last six months to one year by automatically generating different font colors triggered by the date items were published, and will also automatically revert back to the standard font color after the one year mark
- Ability to bookmark pages that individual users need to visit frequently
- Ability to auto-generate a “clickable” table of contents that allows us to add, delete and move sections within the handbook without having to recreate the table of contents
- Ability to link to internal and external websites with unbreakable link feature if sections are moved or updated within the handbook
- Ability to quickly skim through the handbook by adding cursor pop-ups, drop-downs and clickable lists
- Ability to have a search “Find” feature that stays on the screen while viewing any handbook
- Ability to add a search of frequently asked questions and answers
- Ability to add metadata columns for each document, and metadata associated with the handbook will be added and mapped for better search results
- Ability to add audio and video links that provide step-by-step instructions
- Ability to access handbooks from any location without having to create and remember a new user ID and password
- Ability to add screenshots, images, charts, graphs or other media to the handbooks
- Ability to provide access to certain sections or elements of the handbook to external parties via a public facing website linked to our internal facing website

##### **2. Data Reporting Features**

- Real-Time user-friendly reporting with the ability to track handbook usage by staff and/or external parties, enabling the measurement of each handbook’s usage, for example:

###### **Internal Agency Report Features:**

- System report that provides the number of hits\* for each handbook
  - Hits are defined as a request to Contractor’s web-server for a specified Handbook, where users are accessing the page or downloading the document.
- System report that provides the most common program handbook sections being viewed
- System report that provides the most common searches for a specified program handbook

### **External Report Features**

- System report that provides the number of hits for each handbook
- System report that provides the most common program handbook sections being viewed
- System report that provides the most common searches for a specified program handbook

Contractor will provide training, support and professional services in order to train users on the new handbook formats and the new reporting features. Contractor will assume responsibility to ensure that there is a cultural shift in making staff comfortable in utilizing the new system/practices with ease through:

### **3. Training Services**

- Training on new handbook technology for staff who work as publishers/contributors
- Training on migration of existing handbooks to the new system
- Training on ongoing support and maintenance to the new system
- Train-the-Trainer for training all agency staff on how to use the new system
- Retrain specific staff if required
- A brief help document on the use of the new handbook technology will be created and provided for staff

The contractor will provide all the above training deliverables during the user acceptance testing and training phase, detailed below. The contractor will employ best practices to ensure a successful implementation and adoption of the new handbook technology. The training will be provided onsite via web-based meeting sessions.

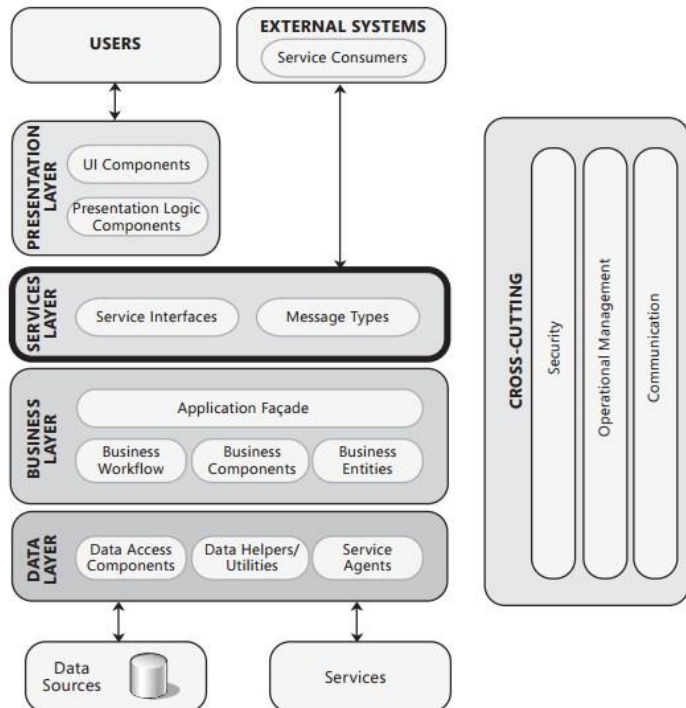
### **B. Technology Components**

The solution design will be based on San Mateo County's existing Office 365 SharePoint Online. A supporting "SharePoint Provider Hosted App" will be setup in Azure for development of components not supported by SharePoint Online. Microsoft Azure will be hosted by Contractor.

- Web-based and Mobil Application implementation
- The code and other resources including image files, CSS, etc.
- Document explaining application setup and basic troubleshooting
- A list of any important usernames and their passwords (for Admin accounts)
- Transfer of Microsoft Azure Cloud Hosting and maintenance service to County of San Mateo (contractor to transition to County of San Mateo (HSA) by September 2020)
- Contractor will work directly with the County's Information Services Department to ensure a smooth transition of Microsoft Azure Cloud Hosting and maintenance service

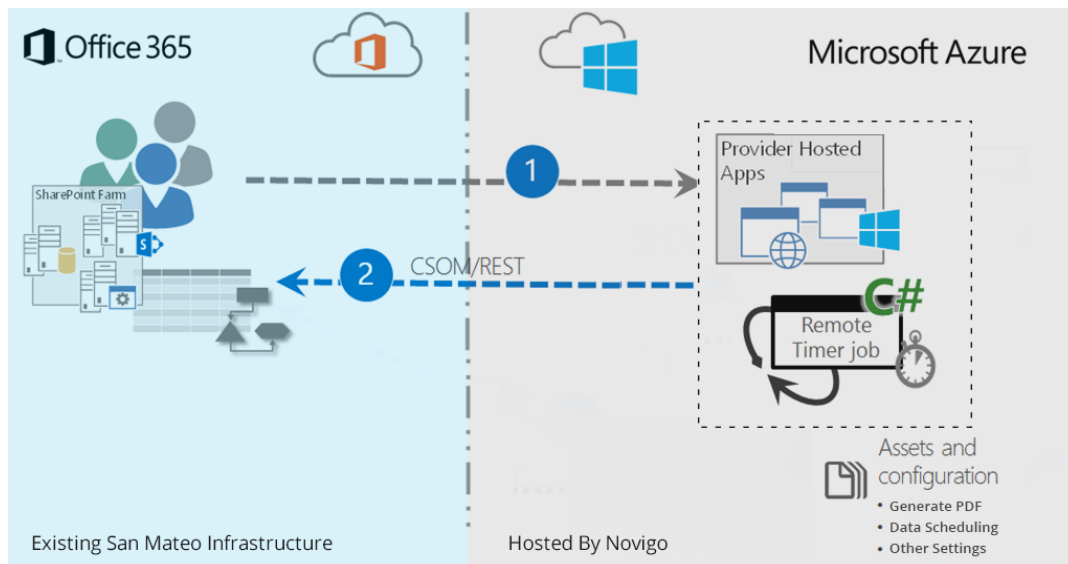
1. The solution will include the following components and related features:

<b>Component</b>	<b>Features</b>
<b>Workflow</b>	Workflow management will provide out of the box functionality to manage workflows within the handbook approval process. Automated notifications, delegations or authority in case of absences or other reasons, etc. can be configured.
<b>Security</b>	Provide mechanism for authentication and authorization.
<b>User Management</b>	Define users and roles and manage permissions. These permissions can then be used to determine particular workgroups that can access internal handbook sites or external handbook site views. The permission settings can also be used

	to ensure varying levels of access to the system. Management levels can be configured to generate reports.
<b>Reporting</b>	Provide dashboard and reports – ad hoc, canned, interactive and auditing reports for external and internal site traffic.
<b>Easy to Use and Friendly Interface</b>	The tool will be developed to be user-friendly and intuitive, making it extremely easy to use. Features like quick access will be designed to help users adopt the system quickly and effortlessly.
<b>Create handbooks within the browser</b>	The system allows creation of rich and modern handbooks from within the browser. The interface will be like Microsoft Word, allowing the users to start creating new handbooks from the system with a minimal learning curve.
<b>Web Application Design Approach</b>	<p>The following picture shows the architecture and design approach that will be followed for designing the web applications:</p>  <pre> graph TD     subgraph Clients         Users[USERS]         ExtSys[EXTERNAL SYSTEMS Service Consumers]     end      subgraph Layers         direction TB         P[PRESENTATION LAYER UI Components Presentation Logic Components]         S[SERVICES LAYER Service Interfaces Message Types]         B[BUSINESS LAYER Application Façade Business Workflow Business Components Business Entities]         D[DATA LAYER Data Access Components Data Helpers/Utilities Service Agents]     end      subgraph CrossCutting [CROSS-CUTTING]         direction TB         Sec[Security]         OM[Operational Management]         Com[Communication]     end      subgraph DataSources [Data Sources]         DS[(Data Sources)]     end     subgraph Services         Svc[Services]     end      Users &lt;--&gt; P     ExtSys &lt;--&gt; S     P &lt;--&gt; S     S &lt;--&gt; B     B &lt;--&gt; D     D &lt;--&gt; DS     D &lt;--&gt; Svc     </pre> <p><b>Presentation Layer:</b> This layer contains the user oriented functionality responsible for managing user interaction with the system, and generally consists of components that provide a common bridge into the core business logic encapsulated in the business layer.</p> <p><b>Service Layer:</b> This layer exposes the business functionality of the application as external service. The service layer effectively provides an alternative view that allows clients to use a different channel to access the application. This allows the application to better support multiple client types, and promotes re-use and higher level compositions of functionality across applications.</p>

	<p><b>Business Layer:</b> This layer implements the core functionality of the system and encapsulates the relevant business logic. It generally consists of components, some of which may expose service interfaces that other callers can use.</p> <p><b>Data Layer:</b> This layer provides access to data hosted within the boundaries of the system and data exposed by other networked systems; perhaps accessed through services. The data layer exposes generic interfaces that the components in the business layer can use.</p>
--	--

2. The solution design will be based on the following logic diagram:



3. The following two stage approach will be applied to the existing handbook documents:

- Stage 1 - Documents that can be recreated into Rich Text Format:
  - Convert all handbooks to rich text format pages with newly designed handbook template
  - Divide all handbooks into several SharePoint pages based on sections or designated pages
  - Create dynamically generated tables of contents for each program handbook by linking each page to a section
  - Create an automatically modifiable table of contents for each document within each program handbook that updates easily as new sections are added or moved or updated
  - Create a way for each individual user to be able to bookmark pages
- Stage 2 – Documents that cannot be recreated into Rich Text Format:
  - Will be maintained in their original format
  - Will be placed in appropriate site collection in accordance with the appropriate program and filed in document libraries

### **C. Office 365 SharePoint Online**

The Contractor's Policy Framework will be deployed on County's Office 365 SharePoint Online. Contractor will use the following hierarchical architecture:

1. Documents related to each program handbook will be uploaded to separate site collections. This will enable users and permission management for each program. This will allow set-up of search filters to show handbooks related to each specific program only
2. The program handbooks and documents that are convertible to the Rich Text Format will be stored in the Pages Library. The Pages Library will be a depository for converted files
3. The handbooks that are not convertible to the Rich Text Format (to be used in the new system) will be retained in their original format and will be stored in document libraries. Independent document libraries will be created for all topics. This will segregate handbooks from different topics into different documents libraries. Content Types, Handbook Templates and Metadata fields will be used in the design to make the system scalable for new programs in the future

### **D. Browser Support**

The solution will be supported using the following browsers:

- Internet Explorer 10+
- Firefox 30+
- Google Chrome 15+

**Note:** Microsoft Edge browser is not 100% HTML5 compliant and may not support all features of the application, and hence is removed from the compatible browser list.

### **E. Software and Hardware Requirements**

A SharePoint Provider Hosted Application will be developed and hosted on Azure by the Contractor. The components that are not possible to be deployed on SharePoint Online will be built and deployed on Azure. Integration between SharePoint Online and Contractor hosted Application will be managed through REST based Services. Contractor will be responsible for implementing the given solution on cloud services provided by Microsoft Azure. The hosting availability and security of all the instances used by Contractor for Cloud implementation are governed by Microsoft Azure SLA.

### **F. Search Configuration**

A custom Advanced Search Web part will be deployed on Office 365 SharePoint Online. The advanced search web part will have the following features:

1. Configurable site scopes – to search for handbooks within individual programs
2. Configure filters scopes – to search for handbooks within topics and additional metadata-based filters
3. Show popular searches
4. Show filters for search drill down

### **G. User Search by Type**

1. **Non-Convertible Handbooks**  
Segregate the Handbooks into different Programs and Topics. Move the PDF / DOC files to newly created SharePoint Document Libraries
2. **Convertible Handbooks**  
Create new pages in Pages Library with configurable metadata fields
3. **To Search Non-Convertible**

- Search results will redirect to actual handbook documents
4. **To Search Convertible Handbooks**  
Search results will redirect to the section within the handbook

#### F. **Policy Management Framework**

Contractor's framework solution is scalable, user-friendly and flexible in managing, approving, updating of handbooks, and policies with pre-defined workflows. Contractor will be able to support up to 500 concurrent users and provide real-time analytics. The solution will work with SharePoint Online (Office 365) and it include the following modules:

1. Customized filterable search results
2. Maintain handbook revision history and logs
3. Automatically updates the Table of Contents, Links and references within the handbooks
4. Bookmarks section within the handbooks
5. Tracks changes in the handbook
6. Provides analytics on usage of handbooks

#### H. **Implementation Timeline**

##### 1. **Detailed Implementation Plan and Timeline:**

The project duration is 21 weeks for design, development, integration and testing, followed by 10 weeks of User Acceptance Testing (UAT) by County. After Go-Live, Contractor will provide free warranty and support for 10 weeks. Post the 10 weeks of free warranty and support, support will be provided on a paid basis.

The UAT duration will be scheduled flexibly so as to ensure that the business users understand the system thoroughly and a smooth shift to the new system takes place. The UAT can be reduced if user onboarding happens before the end of this duration, on the request by County.

Technical analyst will be stationed in Belmont, CA for a period of 12 weeks during the requirement gathering phase and UAT period. The entire design, upgrade, solution development process, handbook to rich text conversion process and support during the free warranty phase will be carried out from offsite.

	Jan					Feb				Mar				Apr				May					Jun				Jul				Aug					Sep			
Week #	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4
Month	Month 1					Month 2				Month 3				Month 4				Month 5					Month 6				Month 7				Month 8					Month 9			
Week Beginning	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	36	37	38	39
Requirements Gathering (Onsite)																																							
Design and Documentation																																							
SharePoint Web Application development - Sprint 1																																							
SharePoint Web Application development - Sprint 2																																							
SharePoint Web Application development - Sprint 3																																							
Contingency Buffer																																							
Documentation & User Manuals																																							
Integration Testing and Final Modifications																																							
UAT & Training HSA Staff (Onsite)																																							
Deployment & Go Live (Onsite)																																							
Free Warranty Support (10 Weeks)																																							
Collect all Documents and Start Processing																																							
Conversion from PDF / DOCX to Rich Text Format																																							
Insert Documents to Upgraded SharePoint System																																							

The effective go-live date is 27 weeks from commencement of work.

<b>Milestone</b>	<b>Timeline*</b>	<b>Deliverable</b>	<b>Sign-Off Criteria</b>
<b>1: Advance</b>	Start of Project	1) Statement of Work 2) Contract Agreement	The County of San Mateo (HSA) and the Contractor will agree to sign off on the deliverables
<b>2: End of Requirements Gathering</b>	Week 1 to Week 6	1) Business Requirements Gathering 2) Design Document and handbook template	The County of San Mateo (HSA) to approve and sign off on the deliverables
<b>3: End of Sprint 2</b>	Week 9 to Week 11	1) UI Prototype 2) Framework Components – Logging, Auditing, Caching, Security 3) SharePoint Schema 4) SharePoint Search Filters 5) SharePoint Document Content Types	The County to San Mateo (HSA) to sign off on the demo deliverables
<b>4: End of Integration Testing</b>	Week 19 to Week 21	1) SharePoint Page Layouts 2) SharePoint Handbook Layouts 3) Integrations 4) Reports	The County of San Mateo (HSA) to sign off on the demo deliverables

<b>5: Conversion of Handbooks to New Template</b>	Week 16 to Week 20	1) Conversion of all Handbooks to the new template design	The County of San Mateo (HSA) to sign off on the New Handbooks template, and at the completion of all handbooks to the new template design
<b>6: Upon Go-Live</b>	Week 27 to Week 28	1) UAT 2) Training of Staff 3) Retraining of Staff if Required 4) Train-the-Trainer for All HSA personnel 5) Migration of handbooks to the system templates 6) User Help Document 7) End User Testing	The County of San Mateo (HSA) to sign off on User Acceptance Testing

<b>Maintenance and Hosting Deliverables</b>	<b>Timeline*</b>	<b>Details</b>	<b>Sign-Off Criteria</b>
<b>Free Warranty</b>	Week 29 to Week 39	1) Provide 10 weeks of warranty on all components of the new handbook technology solution	The County of San Mateo to sign off if no outstanding issues remain unresolved
<b>Annual Maintenance Contract (AMC) – Year 1 + Cloud Hosting</b>	September 1, 2018 to August 31, 2019	1) Ongoing Maintenance 2) Cloud Hosting Microsoft Azure	The County of San Mateo to sign off no outstanding issues remain from year 1 + Cloud Hosting

<b>AMC – Year 2 +Cloud Hosting and Cloud Hosting Transition to San Mateo County</b>	September 1, 2019 to September 30, 2020  Cloud Hosting Transition to occur by September 2020	1) Ongoing Maintenance 2) Cloud Hosting Microsoft Azure 3) Cloud Hosting transition of Microsoft Azure to San Mateo County with no impact to handbook technology services to end user 4) Documentation for integrations between SharePoint & Azure.	The County of San Mateo to sign off on the Cloud Hosting transition by the Contractor to San Mateo County in order to ensure no negative impact occurred to the handbook technology services to the end user
---	--	---	--

*\*Timeline may be adjusted as agreed upon by both parties to meet County's projected goal*

#### **I. Contractor Responsibilities**

Contractor will provide professional services, technical support, and training required to assist in the end-to-end implementation of a new handbook technology system that provides timely accurate search results for all program handbooks. To accomplish this, the Contractor will:

- Configure and capture case elements and program specific information
- Identify root causes and causal factors and maintain this data for historical and trend analysis
- Allow electronic exchange and monitoring of correction of error findings on-time
- Allow for different roles with different permission levels within the system, thereby allowing for varying access to the system
- Configure and set up reports for accuracy rates, monthly/annual trends, specific unit/supervisor/individual accuracy trends and root cause analysis related to quality review, quality control and quality assurance
- Export reports and data into other applications like MS Access, MS Excel and other Business Intelligence Systems
- Single Sign-On Authentication
- Data encryption as per HIPAA guidelines for sensitive data
- Data Migration to the new application
- Assign a maximum of 10 FTE for this project including a Senior Project Manager who will also act as single point of contact
- Provide onsite training for Staff Development Staff on the usage of the handbook technology
- Provide a train-the-trainer to train all HSA personnel on the usage of the technology
- Provide a brief user help document on how to use the new technology
- Provide free warranty on this solution for a period not to exceed 10 weeks
- Provide options for Annual Maintenance and Support (AMC)
- Provide a dedicated email ID for support (Eg: [hsa\\_support@novigosolutions.com](mailto:hsa_support@novigosolutions.com))
- Provide a dedicated and single point of contact for all support needs for the duration of the AMC contract
- Adhere to the Service LA for the duration of the AMC contract

## **J. Maintenance Level and Support**

Contractor shall provide technical support to the application software along with maintenance of deployment server. Maintenance, support and service shall include:

- A dedicated email ID for support ( Eg: [County\\_of\\_San\\_Mateo\\_HandbookTechSupport@novigosolutions.com](mailto:County_of_San_Mateo_HandbookTechSupport@novigosolutions.com))
  - A dedicated single point of contact (SPOC) for all support needs for the duration of the Agreement
  - A senior technical engineer will be assigned as the SPOC for the entire duration of the Annual Maintenance Agreement (AMC) for 3 years
  - The SPOC will be available at all times during San Mateo County's business hours (8 A.M. PST – 5 P.M. PST)
  - In case more clarity is required, the SPOC will arrange for a telephonic conversation with San Mateo County's designated point of contact
  - The SPOC will participate in management, prioritization, minor enhancements, break and fix activities, problem management, stability analysis, etc.
  - The SPOC will have a specific, deep understanding and expertise in the solution
  - The SPOC may have root or administrator access to basic systems
  - Contractor engineers will require approvals for CR management, identifying if an issue is a bug or a new feature and will respond accordingly
1. Support requests are categorized into Priority Levels 1, 2, 3 and 4 based on the type of issue.

**Priority 1:** Issues that cause application breakdown

**Priority 2:** No application breakdown, but an impact to the application's day-to-day usability has been detected

**Priority 3:** Low priority issues/enhancements that are helpful in making it easier for the users to use the system

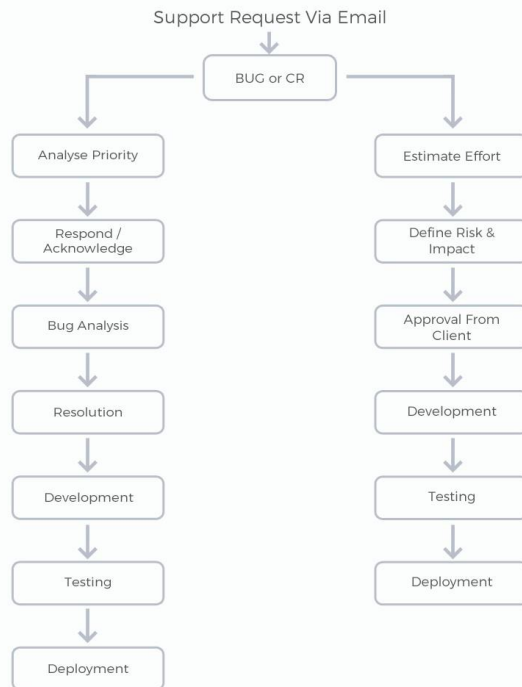
**Priority 4:** Low priority issues/enhancements

Priority	Response Time	Resolution Time
Priority 1	4 Hours	8 Hours
Priority 2	4 Hours	8-12 Hours
Priority 3	8 Hours	24 Hours
Priority 4	18 Hours	40 Hours

## **2. Free Warranty Phase**

- The Contractor will provide a warranty on all the components of the new handbook technology solution under the scope of this document for a period of ten weeks from the date of issuing the acceptance certificate.
- Novigo Solution will provide labor at zero cost during the warranty period.
- County of San Mateo will incur the cost of any hardware pertaining to this project.
- Annual maintenance and support contract (AMC) will be initiated post the warranty phase.

### 3. Diagram of Support Model



### 4. Definition of Bug and Change Request

Every support request will initially be analyzed to understand if it's a Bug or Change Request. The following definitions will be criteria to determine the nature of the support request at hand.

#### 5. Bug Definition

Any error, flow, failure or fault in the developed solution that causes it to produce an incorrect or unexpected result, or behave in unintended way(s), arising from mistakes and errors made in either the developed solution's source code or its design, or in components, will be treated as a Bug.

#### K. Bug Resolution Process

1. **Identify:** Once a bug is identified, the details of the bug is documented for the support person to better understand the problem at hand.
2. **Analyze priority:** The priority of the bug is analyzed and one of the priority levels is assigned to the bug.
3. **Response:** Based on the priority level, the support person will acknowledge and respond via email and/or call as required within the timeline set.
4. **Bug Analysis:** The support person will analyze the reason for the bug and try to understand the effect of the bug on the application.
5. **Resolution:** Once the resolution is found, the resolution is documented and processed. The root cause analysis of the bug is done and the analysis is documented.
6. **Development, Testing & Deployment:** The documented resolution then proceeds to the development stage after successful User Acceptance Testing (UAT), and the bug is deemed to be resolved.

#### Change Request (CR) Definition

Any effort greater than 40-man hours, arising out of a request for a new functionality, enhancements to an existing functionality, changes in underlying platform or a problem report that identifies bugs, be will treated as a CR.

Changes in underlying platform will be any changes in the operating system used by County or in other systems used by County that will be integrating with the current solution.

#### **L. CR Management Process**

- 1. Initiate a CR:** Once a CR is initiated, the details of the CR need to be documented to help understand the changes that need to be implemented in the application.
- 2. Estimate Effort:** The total effort and cost required to implement the change will be estimated during this phase.
- 3. Define Risk & impact:** The impact to the application from the change will be documented and also the risks involved with implementing this change will be listed.
- 4. Approval:** The findings from the previous phases will be presented to County, explaining the necessity, feasibility and effect of the CR on the application. Once County approves the CR, the request proceeds.
- 5. Development, Testing & Deployment:** Once the CR is approved by County, it proceeds to the development stage. After successful UAT, the change is deployed to the application.

Contractor will provide a free warranty on all the components of the solution under the scope of this agreement for a period of 10 (ten) calendar weeks from the date of issuing the acceptance certificate for the warranty. Contractor will also agree to provide labor at zero cost during the warranty period. The cost for Maintenance and Support after the free warranty period, are provided in Exhibit B. Maintenance will be renewable at the start of every year and with the termination of the Agreement. County shall have the option to renew maintenance and support under a new separate agreement upon termination of this Agreement. Any change request by County during this maintenance agreement period will be done on a Time and Materials (T&M) basis, over and above the cost quoted. Costs for change requests will be negotiated by the County and approved in writing.

#### **Support Activities**

- Respond to user queries as per the Service Level Agreement timeline
- Investigate root cause and fix the issues as reported
- Fix bugs as reported
- Help and train the publishers of the handbooks and the training team in using the system
- Resolve any Ad-Hoc issues reported
- Install and configure system software
- Upgrade system software and systems configurations
- Use control panel software to make system changes
- Track issues through log files
- Tweak software and system configurations
- Find the cause of server load problems
- Restart services
- System hardening and hack prevention and cure
- Custom kernel compilations, if required
- Analyze system problems and recommend solutions

A dedicated personnel of the Contractor will be appointed, who will attend to all queries raised by the County by email. The support engineer will be available during the business hours of the County (8 A.M. PST to 5 P.M. PST).

**County's option to request additional services and modify services under this Agreement**

County shall have the option to request additional related services or modify services described in this agreement. Additional services or modification requests will be in writing to the Contractor and agreed upon by both parties. Contractor shall be entitled to payment for all services performed prior to a modification of service request at contract current rates. Modification requests on additional services will be determined and may result in additional charges to the County.

**(End of Exhibit A1)**

**Exhibit B1 Handbook**  
**Payments and Rates**

**A. Services**

1. Contractor will invoice County upon completion of each milestone shown in the services payment table below for actual cost incurred.
2. County shall pay Contractor upon receipt and approval of invoices along with appropriate documentation.
3. The total cost for service milestones detailed below, including any taxes or fees, shall not exceed **ONE HUNDRED SEVENTY FOUR THOUSAND DOLLARS (\$174,000)**.

**Service Payment Table:**

Payment Terms	Milestone	Amount not to e(USD)	Percentage (%)
Milestone -1/Advance	Start of Project	\$33,600	20%
Milestone-2/End of Requirements Gathering	End of Week 6	\$33,600	20%
Milestone-3/End of Sprint 2	End of Week 11	\$42,000	25%
Milestone-4/End of Integration Testing	End of Week 21	\$33,600	20%
Milestone-5 and 6 Conversion of Handbook to New Template and Go-Live	End of Week 28	\$25,200	15%
<b>Total – Solution Development</b>		<b>\$168,000</b>	<b>100%</b>

Payment Terms	Milestone	Amount (USD)	Percentage (%)
Completion of Optional Scope (conversion of existing documents)	End of Week 26	\$6,000	100%
<b>Total – Optional Scope</b>		<b>\$6,000</b>	<b>100%</b>
<b>Total – Solution Development and Optional Scope</b>		<b>\$174,000</b>	

**B. Annual Maintenance, Cloud Hosting and Cloud Hosting Transition**

1. Contractor shall invoice County annually for Maintenance, Cloud Hosting and the Cloud Hosting Transition for actual cost incurred based on the terms shown in the Maintenance and Hosting Payment table.
2. County shall pay Contractor upon receipt and approval of invoices.
3. The total cost for Maintenance, Cloud Hosting and the Cloud Hosting Transition including taxes and fees shall not exceed **ONE HUNDRED FIFTEEN THOUSAND DOLLARS (\$115,000)**.
4. The total cost for all services under Exhibit B1, including any taxes and fees, shall not exceed **TWO HUNDRED EIGHTY NINE THOUSAND DOLLARS (\$289,000)**.

**Maintenance and Hosting Payment table:**

Payment Terms	Milestone	Amount (USD)
Free Warranty	Week 29 to Week 39	Free
AMC + Cloud Hosting – Year 1	September 1, 2018 to August 31, 2019	\$60,000
AMC, Cloud Hosting and Cloud Hosting & Maintenance Transition to San Mateo County ISD – Year 2 (transition to San Mateo County to occur by September 30, 2020	September 1, 2019 to September 30, 2020	\$55,000
<b>Total – AMC, Cloud Hosting and Cloud Hosting Transition</b>		<b>\$115,000</b>
<b>Grand Total</b>		<b>\$289,000</b>

County shall have the option to adjust funding across line items in the Milestones shown in above and across fiscal years as agreed upon by both parties and approved by the County in writing as long as it does not exceed the total Agreement obligation.

**(End of Exhibit B)**

**Exhibit C**  
**Performance Monitoring**

Services described in Exhibit A1 and payments described in Exhibit B1 provided under this amended Agreement are subject to performance monitoring. The Contractor shall comply with the following performance standards:

Performance Activity	Performance Standard
Application Availability	99% of the time is operational, functional and usable.
Application Maintainability	At all phases of the software development, will follow the same development standards.
Support Quality	Bug fixes / changes request implementation will follow the same rigorous quality checks as followed in development.
Release Quality within user acceptance testing (UAT)	During the UAT phase, the issues identified will be resolved by following the same rigorous quality checks as followed in development.
Deliverable(s) produced in Change Request Delivered to UAT on Schedule	Deliverable(s) produced in Change Request and included in a release shall be delivered to UAT no later than the baseline planned Release to UAT date set forth in Release Work Plan.
Bug Resolution Timelines	Performance standard will adhere to the standards defined in Exhibit A Service Level response times.
Disaster Recovery	<p>Verify annually that disaster recovery procedures and facilities exist and that tests have been performed to allow for alternate means of System Availability within 24 hours in the event a Disaster has been declared for the Central Site Facility.</p> <p>DR for application is ensured by adopting geo-replication feature in cloud, which maintains instances in different geographical locations and is handled by Microsoft Azure.</p>

**(End of Exhibit C)**

**Attachment P**  
**Personally Identifiable Information**  
**Requirements for County Contractors, Subcontractors, Vendors and Agents**

**I. Definitions**

Personally Identifiable Information (PII), or Sensitive Personal Information (SPI), as used in Federal information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII may only be used to assist in the administration of programs in accordance with 45 C.F.R. § 205.40, *et seq.* and California Welfare & Institutions Code section 10850.

- a. **“Assist in the Administration of the Program”** means performing administrative functions on behalf of County programs, such as determining eligibility for, or enrollment in, and collecting context PII for such purposes, to the extent such activities are authorized by law.
- b. **“Breach”** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to context PII, whether electronic, paper, verbal, or recorded.
- c. **“Contractor”** means those contractors, subcontractors, vendors and agents of the County performing any functions for the County that require access to and/or use of PII and that are authorized by the County to access and use PII.
- d. **“Personally Identifiable Information” or “PII”** is personally identifiable information that can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. PII may be electronic, paper, verbal, or recorded.
- e. **“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the County or County's Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the County, on behalf of the County.
- f. **“Secure Areas”** means any area where:
  - i. Contractors administer or assist in the administration of County programs;
  - ii. PII is used or disclosed; or
  - iii. PII is stored in paper or electronic format.

## **II. Restrictions on Contractor re Use and Disclosure of PII**

- a. Contractor agrees to use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50, *et seq.* and California Welfare & Institutions Code section 10850 or as otherwise authorized or required by law. Disclosures, when authorized or required by law, such as in response to a court order, or when made upon the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by the County. No Contractor shall duplicate, disseminate or disclose PII except as allowed in this Agreement.
- b. Contractor agrees to only use PII to perform administrative functions related to the administration of County programs to the extent applicable.
- c. Contractor agrees that access to PII shall be restricted to Contractor's staff who need to perform specific services in the administration of County programs as described in this Agreement.
- d. Contractor understands and agrees that any of its staff who accesses, discloses or uses PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions available under applicable Federal and State laws and regulations

## **III. Use of Safeguards by Contractor to Protect PII**

- a. Contractor agrees to ensure that any agent, including a subcontractor, to whom it provides PII received from, or created or received by Contractor on behalf of County, agrees to adhere to the same restrictions and conditions contained in this Attachment PII.
- b. Contractor agrees to advise its staff who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable Federal and State laws and regulations.
- c. Contractor agrees to train and use reasonable measures to ensure compliance by Contractor's staff, including, but not limited to (1) providing initial privacy and security awareness training to each new staff within thirty (30) days of employment; (2) thereafter, providing annual refresher training or reminders of the PII privacy and security safeguards to all Contractor's staff; (3) maintaining records indicating each Contractor's staff name and the date on which the privacy and security awareness training was completed; and (4) retaining training records for a period of three (3) years after completion of the training.

- d. Contractor agrees to provide documented sanction policies and procedures for Contractor's staff who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment when appropriate.
- e. Contractor agrees that all Contractor's staff performing services under this Agreement sign a confidentiality statement prior to accessing PII and annually thereafter. The signed statement shall be retained for a period of three (3) years, and the statement include at a minimum: (1) general use; (2) security and privacy safeguards; (3) unacceptable use; and (4) enforcement policies.
- f. Contractor agrees to conduct a background check of Contractor's staff before they may access PII with more thorough screening done for those employees who are authorized to bypass significant technical and operational security controls. Contractor further agrees that screening documentation shall be retained for a period of three (3) years following conclusion of the employment relationship.
- g. Contractor agrees to conduct periodic privacy and security reviews of work activity, including random sampling of work product by Contractor's staff by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of County's programs and the use and disclosure of PII. Examples include, but are not limited to, access to data, case files or other activities related to the handling of PII.
- h. Contractor shall ensure that PII is used and stored in an area that is physically safe from access by unauthorized persons at all times and safeguard PII from loss, theft, or inadvertent disclosure by securing all areas of its facilities where Contractor's staff assist in the administration of the County's programs and use, disclose, or store PII.
- i. Contractor shall ensure that each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee of Contractor and access is revoked.
- j. Contractor shall ensure that there are security guards or a monitored alarm system at all times at Contractor's facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.
- k. Contractor shall ensure that data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only those authorized by this Agreement. Visitors to any Contractor data centers area storing PII as a result of administration of a County program must be escorted at all times by authorized Contractor's staff.

- l. Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which Contractor staff can transport PII, as well as the physical security requirements during transport.
- m. Contractor shall ensure that any PII stored in a vehicle shall be in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.
- n. Contractor shall ensure that PII shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.
- o. Contractor shall ensure that all workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- p. Contractor shall ensure that servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- q. Contractor agrees that only the minimum necessary amount of PII required to perform required business functions will be accessed, copied, downloaded, or exported.
- r. Contractor shall ensure that all electronic files, which contain PII data is encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- s. Contractor shall ensure that all workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily. In addition, Contractor shall ensure that:
  - i. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.

- ii. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
  - iii. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
  - iv. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.
- t. Contractor shall ensure that all of its staff accessing Personally Identifiable Information on applications and systems will be issued a unique individual password that is a least eight (8) characters, a non-dictionary word, composed of characters from at least three (3) of the following four (4) groups from the standard keyboard: upper case letters (A-Z); lower case letters (a-z); Arabic numerals (0-9) and special characters (!, @, #, etc.). Passwords are not to be shared and changed if revealed or compromised. All passwords must be changed every (90) days or less and must not be stored in readable format on the computer or server.
- u. Contractor shall ensure that usernames for its staff authorized to access PII will be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty- four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
- v. Contractor shall ensure when no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the Personally Identifiable Information cannot be retrieved.
- w. Contractor shall ensure that all of its systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.
- x. Contractor shall ensure that all of its systems providing access to PII must display a warning banner stating, at a minimum that data is confidential; systems are logged, systems use is for business purposes only by authorized users and users shall log off the system immediately if they do not agree with these requirements.
- y. Contractor will ensure that all of its systems providing access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII. The audit trail shall be date and time stamped; log both successful and failed accesses be read-access only; and be restricted to authorized users. If PII is stored in a database, database logging functionality shall be enabled. The audit trail data shall be archived for at least three (3) years from the occurrence.

- z. Contractor shall ensure that all of its systems providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.
- aa. Contractor shall ensure that all data transmissions of PII outside of its secure internal networks must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used. Encryption can be end to end at the network level, or the data files containing PII can be encrypted. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.
- bb. Contractor shall ensure that all of its systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.
- cc. Contractor shall ensure that audit control mechanisms are in place. All Contractor systems processing and/or storing Personally Identifiable Information must have a least an annual system risk assessment/security review that ensure administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection. Review shall include vulnerability scanning tools.
- dd. Contractor shall ensure that all of its systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.
- ee. Contractor shall ensure that all of its systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.
- ff. Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.
- gg. Contractor shall ensure its data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.
- hh. Contractor shall establish documented procedures to backup PII to maintain retrievable exact copies of PII. The documented backup procedures shall contain a schedule which includes incremental and full

backups, storing backups offsite, inventory of backup media, recovery of PII data, an estimate of the amount of time needed to restore PII data.

- ii. Contractor shall ensure that PII in paper form shall not be left unattended at any time, unless it is locked space such as a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information. Locked spaces are defined as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use, meaning that there are Contractor's staff and non-Contractor functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities
- jj. Contractor shall ensure that any PII that must be disposed of will be through confidential means, such as cross cut shredding or pulverizing.
- kk. Contractor agrees that PII must not be removed from its facilities except for identified routine business purposes or with express written permission of the County.
- ll. Contractor shall ensure that faxes containing PII shall not be left unattended and fax machines shall be in secure areas. Faxes containing PII shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender. All fax numbers shall be verified with the intended recipient before send the fax.
- mm. Contractor shall ensure that mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery.

#### **IV. Reporting of Breaches Required by Contractor to County; Mitigation**

- a. Contractor shall report to County within one business day of discovery, to the County contact listed in this agreement by email or telephone as listed in the of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement.
- b. Contractor understands that State and Federal Law requires a breaching entity to notify individuals of a breach or unauthorized disclosure of their PII. Contractor shall ensure that said notifications shall comply with the requirements set forth in California Civil Code section 1798.29, and 42 U.S.C. section 17932, and its implementing regulations, including but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than sixty (60) calendar days from the date of the breach/the breach was discovered?.

- c. Contractor agrees to promptly mitigate, to the extent practicable, any harmful effect that is known to Contractor stemming from a use or disclosure of PII in violation of the requirements of this Agreement, including taking any action pertaining to such use or disclosure required by applicable Federal and State laws and regulations.

#### **V. Permitted Uses and Disclosures of PII by Contractor**

Except as otherwise limited in this schedule, Contractor may use or disclose Personally Identifiable Information to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement; provided that such use or disclosure would not violate the Privacy Rule if done by County.

#### **VI. Obligations of County**

- a. County shall provide Contractor with the notice of privacy practices that County produces in accordance with California Welfare and Institutions Code section 10850, as well as any changes to such notice.
- b. County shall notify Contractor of any changes in, or revocation of, permission by Individual to use or disclose PII, if such changes affect Contractor's permitted or required uses and disclosures.
- c. County shall notify Contractor of any restriction to the use or disclosure of PII that County has agreed to in accordance with California Welfare and Institutions Code section 10850.

#### **VII. Permissible Requests by County**

County shall not request Contractor to use or disclose PII in any manner that would not be permissible under the Privacy Rule if so requested by County, unless Contractor will use or disclose PII for, and if the Agreement provides for, data aggregation or management and administrative activities of Contractor.

#### **VIII. Duties Upon Termination of Agreement**

- a. Upon termination of the Agreement, for any reason, Contractor shall return or destroy all PII received from County, or created, maintained, or received by Contractor on behalf of County that Contractor still maintains in any form. This provision shall apply to PII that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of the PII.
- b. In the event that Contractor determines that returning or destroying PII is infeasible, Contractor shall provide to County notification of the conditions that make return or destruction infeasible. Upon mutual Agreement of the Parties that return or destruction of PII is infeasible, Contractor shall extend the protections of the Agreement to such PII and limit further uses

and disclosures of such PII to those purposes that make the return or destruction infeasible, for so long as Contractor maintains such PII.

#### **IX. Miscellaneous**

- a. **Regulatory References.** A reference in this Attachment to a section in the Personally Identifiable Information Privacy Rule means the section as in effect or as amended, and for which compliance is required.
- b. **Amendment.** The Parties agree to take such action as is necessary to amend this Schedule from time to time as is necessary for County to comply with the requirements of the Privacy Rule and in accordance 45 CFR § 205.40, *et seq.* and California Welfare and Institutions Code section 10850.
- c. **Survival.** The respective rights and obligations of Contractor under this Attachment shall survive the termination of the Agreement unless and until the PII is destroyed or returned to the County.
- d. **Interpretation.** Any ambiguity in any provision in this Attachment shall be resolved in favor of a meaning that permits County to comply with the Privacy Rule.
- e. **Reservation of Right to Monitor Activities.** County reserves the right to monitor the security policies and procedures of Contractor.