

CLOUD SUBSCRIPTION SERVICES AGREEMENT

This Cloud Subscription Services Agreement ("Agreement") is dated effective February 1, 2019 ("Effective Date"), and is between **Saba Software, Inc.** ("Saba"), a Delaware corporation with an address at 4120 Dublin Boulevard, Dublin, California 94568 USA and the **County of Sonoma, California**, a public entity acting by and through its duly appointed representative ("County"), having a principal address at 575 Administration Drive, Santa Rosa, CA 95403 USA. The Agreement sets forth the terms and conditions under which the parties agree that County may, pursuant to one or more separately executed Orders, subscribe to use the Subscription Services listed on the relevant Order(s).

1. Definitions.

Affiliates means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject.

Content means all electronic content, information, and data submitted to and stored in the Subscription Services by or on behalf of County.

Order means a Saba sales order or Statement of Work executed by Saba and County (or a County Affiliate) that is made pursuant to this Agreement. The Order and the Statement of Work existing as of the date of this Agreement are attached as Exhibit 1 and Exhibit 2.

Policies and Entitlements Page means the page on Saba's website that contains the policies and provisions applicable to the Services, located at <https://policy.saba.com> and incorporated by reference herein. The Saba Cloud Entitlements, Saba Customer Privacy Policy, Information Security Policy, Disaster Recovery and Business Continuity Policy, and Saba Cloud Support Policy, as of the Effective Date, are attached as **Attachments 1, 2, 3, 4 and 5** respectively and incorporated by reference herein. Any changes to the policies and entitlements, when taken as a whole, will not (except as required by applicable law or regulation) operate to diminish the level of Services, rights, and assurances provided to County hereunder.

Subscription Services means the online, standard Web-based application services made generally available by Saba on a subscription basis and identified on the applicable Order.

Service(s) means the Subscription Services and/or any other services identified on the applicable Order.

Subscription Term means the term set forth in the applicable Order, including, without limitation, the initial subscription term, or any renewal subscription term agreed by the parties.

User means an individual with credentials issued by County to log on to the Subscription Services, as more fully described in the applicable Order.

2. Delivery of Subscription Services.

2.1 Subscription Services. During the applicable Subscription Term, Saba will make the Subscription Services available to County, and hereby grants County the right to permit Users to use the Subscription Services in accordance with this Agreement. County may view important information concerning the rights and restrictions associated with each Order on the Policies

and Entitlements Page. The Subscription Services are provided as software-as-a-service and are not customized to County's unique requirements. From time to time throughout the Subscription Term, Saba may make upgrades, changes and/or improvements to the Subscription Services in order to enhance the Subscription Services generally and/or remedy any issues with the Subscription Services.

2.2 Term. The initial Subscription Term for the Subscription Services will be for three (3) years as specified on an Order. Thereafter, the Subscription Services may be renewed for two additional twelve (12) month terms at the County's option. The County will provide written notice of renewal or non-renewal to Saba sixty (60) days prior to the end of the then-current Subscription Term.

2.3 Support. The support policy(ies) for the relevant Subscription Services are available on the Policies and Entitlements Page. Saba maintains self-service, password-protected support websites, which are available 24x7. Each site contains updated County support information. Saba County Support is provided in English only. County Support hours, support telephone numbers, scheduled maintenance windows, and other provisions regarding support of the Subscription Services are posted on the relevant support website and/or in the relevant support policy. Saba may change its scheduled maintenance periods by providing 30-day advance email notification. If necessary but unscheduled maintenance is required, Saba will use reasonable efforts to issue a timely email warning.

2.4 Monitoring. Saba will monitor the Subscription Services, on a 24 x 7 x 365 basis, for correct operation, capacity, and performance. When any faulty operation, capacity, or performance of the Subscription Services is identified and verified by Saba, Saba will endeavor to correct any such issues and restore normal operation of the Subscription Services.

2.5 Privacy and Security. Saba is committed to protecting the personal information that Saba receives from County. As further described in Saba's Customer Privacy, Information Security and Disaster Recovery/Business Continuity Policies (each as available on the Policies and Entitlements Page), Saba will take commercially reasonable and appropriate technical and organizational measures to protect County's personal information against unauthorized access, accidental loss or damage, and unauthorized destruction. Saba and County agree to rely on the penetration tests periodically performed by Saba, in accordance with the Information Security Policy. The security provided by Saba shall be in accordance with good industry practices relating to protection of the types of data typically utilized in the Subscription Services by Saba customers.

2.5.1 Representation, Warranty, and Responsibility as to Data Security.

- a. **Data Security:** Saba shall preserve, and shall ensure that its sub-contractors or vendors preserve, the confidentiality, integrity, and availability of County data with administrative, technical and physical measures that conform to generally recognized industry standards and practices that Saba applies to customers of the Services generally. As further described in the Information Security policy, maintenance of a secure processing environment includes, but is not limited to, the timely application of patches, fixes, and updates to operating systems and

applications as provided by Saba and/or its sub-contractors or vendors. Saba agrees to, and shall ensure that its sub-contractors or vendors comply with the Information Security Policy.

- b. **Encryption Requirements:** The Subscription Services shall encrypt confidential information in transit, including but not limited to Personally Identifiable Information (PII).
- c. **Security Breach:** Saba shall comply, and shall ensure that its sub-contractors or vendors comply, with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information (PII) or other event requiring notification. In the event of a breach, or other event requiring notification under applicable law, Saba shall:
 - (1) Make all commercially reasonable efforts to notify the County by telephone and e-mail within seventy-two (72) hours of any actual breach of security, intrusion, or unauthorized use or disclosure of information of which Saba or its agents become aware and/or any actual use or disclosure of data in violation of any applicable federal or state laws or regulations.
 - (2) Assume responsibility for informing all such individuals in accordance with applicable federal or state laws or regulations.
 - (3) Pursuant to Article 8 of the Agreement, provide indemnity and other protection as specified therein.
- d. **Request to Audit:** Saba will accommodate and upon reasonable notice by Sonoma County (not less than ten (10) business days' notice, and not more often than once (1x) in any twelve (12) month period), work with Sonoma County and/or its subcontractors to submit to a random information security audit. This is to ensure that Saba is providing the Subscription Services in accordance with Saba's information security practices or standards. Saba shall ensure that its sub-consultants and vendors comply with this requirement.
- e. **Cyber Risk Insurance Requirements:** Saba shall include, and shall ensure that its sub-contractors or vendors include, cyber risk insurance requirements in compliance with County of Sonoma Risk Management standards attached hereto as Attachment 6.

2.6 Other Services. Saba may provide related Services (including consulting and training Services) under the terms of this Agreement, as agreed to in writing by the parties and specified on one or more separately executed Orders made subject to this Agreement. Any deliverables provided by Saba in connection with such Services shall only be used in connection with County's authorized use of the Subscription Services. Unless otherwise expressly agreed in writing by the parties, such Services shall be provided on a time and materials basis at Saba's then-current standard rates.

2.7 County's Affiliates. County's Affiliates may purchase Services subject to the terms of this Agreement by executing an Order with Saba under which Affiliate will be bound as County hereunder.

2.8 Users. User subscriptions are for designated Users and cannot be shared or used by more than one User but may be reassigned to new Users replacing former Users who no longer require use of the Subscription Services. The maximum number of Users and/or other subscriptions of the Services is as set forth in the applicable Order. If County wishes to add additional subscriptions for Users or other items, these subscriptions must be purchased in advance of use. Saba may, from time to time and at its own expense, review County's usage of the Services to determine County's compliance with the terms of each Order. Saba will promptly notify County if Saba determines that County's usage of the Services exceeds County's subscribed entitlements. County will pay for any additional subscriptions required for County's actual usage.

2.9 Content Processing. County shall act as the data controller for any and all Content. Saba shall act as the data processor on behalf of County with respect to such Content and shall carry out the instructions of County with regard to the collection, processing, and protection of such Content in accordance with this Agreement.

3. Intellectual Property.

3.1 Content. As between County and Saba, all right, title, and interest in and to the Content is owned exclusively by County. County hereby grants to Saba the right to access and use the Content, solely as reasonably necessary to provide the Services. County shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership of and right to collect, use, process and transmit all Content, and acknowledges that Saba exercises no control whatsoever over any data passing through County's site(s) (including any Content). Saba provides only storage, processing, and delivery services for Content, and is not the publisher of Content. County is responsible for all activity in User accounts.

3.2 Saba Intellectual Property Rights. All right, title and interest in and to the Services (including, without limitation, all intellectual property rights therein and all modifications, extensions, customizations, scripts or derivative works of the Services provided or developed by or for Saba) is owned exclusively by Saba or its licensors. If County or any Users provide Saba with any suggestions, enhancement requests, recommendations or other feedback ("Feedback") regarding the Services, County also grants to Saba a perpetual, irrevocable, worldwide, royalty-free, fully paid up, transferable and sub-licensable license to use, modify, distribute and incorporate County's Feedback into the Services without attribution of any kind. All Feedback, if any, is provided by County without warranties. County shall have no obligation to provide Feedback.

3.3 Restrictions. Saba and County each agree not to derive, or attempt to derive, directly or indirectly, source code or other trade secrets from the other party, or otherwise reverse

engineer or decompile all or any portion of the other party's technology, except and only to the extent expressly permitted by, and in accordance with, applicable law.

4. Representations and Warranties.

4.1 Mutual Representation and Warranties. Each party represents and warrants to the other that (i) it has the legal right and authority to enter into this Agreement and perform its obligations hereunder, (ii) it will not introduce into the Subscription Services any virus, worm, Trojan horse, time bomb, or other malicious or harmful code, and (iii) the performance of its obligations hereunder and delivery and use of the Services will not violate any applicable laws or regulations including without limitation those related to privacy, security, and/or the collection, use, transmission and/or retention of data within or between any jurisdiction(s). With respect to the representation and warranty set forth in (iii) above, Saba's representation relates solely to its delivery of the Services and County's representation relates solely to its and the Users' use of the Services.

4.2 Saba Product Warranty. Saba warrants that the Subscription Services will conform in all material respects with Saba's standard end user documentation for such Subscription Services. In the event of a breach of the warranty set forth in this Section 4.2, County's sole and exclusive remedy will be that Saba shall, upon receipt of written notice of breach, make diligent efforts to become compliant with the warranty set forth in this Section 4.2, and if Saba does not do so within a reasonable period of time, County will be entitled to terminate this Agreement pursuant to Section 10.1.

4.3 Service Level Warranty. Saba warrants that the Subscription Services will perform in accordance with and subject to the Saba Service Level Agreement ("Service Level Agreement" or "SLA"), which is attached hereto as Exhibit 3 and incorporated herein by reference. The SLA states County's sole and exclusive remedy for any breach of the warranty set forth in this Section 4.3.

4.4 Certification under Privacy Shield. Saba represents and warrants to County that Saba is and shall remain certified under the EU-US Privacy Shield Framework managed by the U.S. Department of Commerce, International Trade Administration, or such other comparable framework that the relevant government authorities may institute.

4.5 NO OTHER WARRANTY. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS SECTION 4, THE SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, AND COUNTY'S USE OF THE SERVICES IS AT COUNTY'S OWN RISK. SABA DOES NOT MAKE, AND HEREBY DISCLAIMS, ANY AND ALL OTHER EXPRESS AND/OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. SABA DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE.

4.6 DISCLAIMER OF ACTIONS CAUSED BY AND/OR UNDER THE CONTROL OF THIRD PARTIES. SABA DOES NOT AND CANNOT CONTROL THE FLOW OF DATA TO OR FROM SABA'S NETWORK

AND OTHER PORTIONS OF THE INTERNET. ACCORDINGLY, SABA DISCLAIMS ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO A FAILURE IN THE PERFORMANCE OF INTERNET SERVICES PROVIDED OR CONTROLLED BY A THIRD PARTY OTHER THAN ANY CONTRACTOR OR AGENT OF SABA HEREUNDER.

5. County Obligations. County shall not, and shall procure that Users do not, use the Subscription Services (i) to perform any activity that is unlawful, or that is harmful to or interferes with any use of the Subscription Services, or the network, systems and/or facilities of Saba or the network, systems and/or facilities of any other provider; (ii) to store, process, publish or transmit any threatening, infringing or offensive material, or material that constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of any party's privacy, intellectual property or other rights; (iii) in a service bureau, outsourcing, renting, sublicensing or time-sharing capacity, or in a manner that permits concurrent use of a single User login; (iv) to perform any activity intended to circumvent the security measures of Saba or any third party; or (v) other than in connection with County's products or services. If County becomes aware of any breach of the foregoing, County will notify Saba and remedy the situation immediately, including, if necessary, limiting, suspending or terminating any relevant User's access to the Subscription Services. In the event of a breach or suspected breach of any of the foregoing prohibitions, Saba reserves the right to suspend County's Services, if reasonably necessary to prevent harm to Saba, County, other customers, and/or Saba's partners, vendors, and suppliers with such notice as may be reasonable in the context of the prospective harm. County is responsible for the confidentiality and use of Users' passwords and user names.

6. Fee and Payment Terms.

6.1 Fees and Payment. County will pay to Saba the fees and charges set forth on the Orders. Except as otherwise expressly stated in the applicable Order, all amounts are due within thirty (30) days of County's receipt of Saba's invoice. Any payment by credit card requires Saba's pre-approval and is payable upon signature of the Order. Pricing is subject to change upon renewal or extension of an Order. Except as otherwise expressly set forth herein, all payments are non-refundable.

6.2 Taxes. County will reimburse Saba for all sales, use, excise, and property taxes, value-added tax (VAT), goods and services tax (GST), or other taxes, levies, duties or withholdings Saba is required to collect or remit to applicable tax authorities (except for any taxes based on Saba's net income). If County is required by any applicable law to deduct or withhold amounts otherwise payable to Saba hereunder, County will pay the required amount to the relevant governmental authority, provide Saba with an official receipt or certified copy or other documentation acceptable to Saba evidencing the payment, and pay to Saba, in addition to the payment to which Saba is otherwise entitled under this Agreement, such additional amount as is necessary to ensure that the net amount actually received by Saba free and clear of all taxes

equals the full amount Saba would have received had no such deduction or withholding been required.

7. Limitations of Liability and Allocation of Risk

7.1 LIMITATIONS OF LIABILITY. EXCEPT FOR A PARTY'S OBLIGATIONS UNDER SECTION 8 (DUTY TO DEFEND); OR DAMAGES ARISING OUT OF A PARTY'S FRAUD, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR VIOLATION OF APPLICABLE LAW, OR ANY PERSONAL INJURY OR DEATH TO THE EXTENT CAUSED BY A PARTY; OR ANY LOSS OR DAMAGE FOR WHICH LIABILITY CANNOT BE LIMITED OR EXCLUDED BY APPLICABLE LAW, IN NO EVENT, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT OR OTHERWISE, WILL EITHER PARTY, ITS LICENSORS, OR ITS AFFILIATES, OR THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES OR CONTRACTORS BE LIABLE TO THE OTHER PARTY FOR: (I) ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING WITHOUT LIMITATION ECONOMIC LOSS, LOST PROFITS, LOSS OF USE, REPROCUREMENT COSTS OR LOST OR DAMAGED DATA, EVEN IF SAID PARTY OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF SUCH DAMAGES ARE FORESEEABLE, OR IF SUCH DAMAGES ARISE FROM ANY MISREPRESENTATION, BREACH OF ANY IMPLIED OR EXPRESS WARRANTY OR CONDITION, OR BREACH OF ANY OTHER TERM (INCLUDING A FUNDAMENTAL BREACH OR BREACH OF A FUNDAMENTAL TERM), OR BREACH OF STATUTORY DUTY; OR (II) A MAXIMUM AGGREGATE LIABILITY IN ANY CLAIM, ACTION, DEMAND OR PROCEEDING WHICH EXCEEDS THE TOTAL AMOUNT OF THE FEES ACTUALLY PAID TO SABA BY COUNTY FOR THE SERVICE(S) GIVING RISE TO THE CLAIM DURING THE YEAR IN WHICH CLAIM AROSE.

7.2 ALLOCATION OF RISK. THE PROVISIONS OF THIS AGREEMENT ALLOCATE THE RISKS BETWEEN SABA AND COUNTY. THE FEES PAYABLE BY COUNTY REFLECT THIS ALLOCATION OF RISK, AS EXPRESSED BY THE LIMITED WARRANTIES, REMEDIES AND LIMITATIONS OF LIABILITY SET OUT IN THIS AGREEMENT. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, COUNTY AGREES THAT IT HAS NOT RELIED ON ANY INDUCEMENT, REPRESENTATION, WARRANTY OR STATEMENT MADE BY OR ON BEHALF OF SABA IN RELATION TO THE SUBJECT MATTER OF THIS AGREEMENT. EACH OF THE PARTIES HERETO IRREVOCABLY WAIVES ITS RIGHT TO A JURY TRIAL OF ANY CLAIM OR CAUSE OF ACTION BASED UPON OR ARISING OUT OF THIS AGREEMENT OR ANY DEALINGS BETWEEN THE PARTIES RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT. EACH OF THE PARTIES HERETO ACKNOWLEDGES THAT THIS WAIVER IS A MATERIAL INDUCEMENT TO ENTER INTO THIS AGREEMENT. IN THE EVENT OF LITIGATION, THIS AGREEMENT MAY BE FILED AS A WRITTEN CONSENT TO A TRIAL BY THE COURT.

8. Duty to Defend.

8.1 Saba shall indemnify and defend or settle, at its expense, any claim or action ("Claim") against County that (a) the Subscription Services, as made available by Saba to County under this Agreement and used within the scope of this Agreement, infringe any copyright, trade secret, patent or other proprietary right, or (b) is a result of personal injury or death caused by Saba's negligence or willful misconduct; and Saba shall pay all final judgment awards against County or settlement costs in connection with such Claim.

8.2 County shall defend or settle, at County's expense, any Claim brought against Saba that (a) any Content infringes any copyright, trade secret, patent or other proprietary right of a third party, or (b) is a result of personal injury or death caused by County's negligence or willful misconduct; and County shall pay all final judgment awards against Saba or settlement costs in connection with such Claim.

8.3 As a condition to the defense and settlement obligations of the parties in this Section 8, a party must provide the defending party prompt notice of any Claim and shall cooperate in all reasonable respects with the defending party in connection with any such Claim. The defending party shall be solely entitled to control the handling of any such Claim and to defend or settle any such Claim, in its sole discretion, with counsel of its own choosing.

8.4 With respect to any Subscription Services that are found to be infringing, or in Saba's opinion are likely to be found infringing, Saba may, at its option, (a) obtain the right for County to continue using the Subscription Services; (b) replace or modify the Subscription Services so they are no longer infringing but still provide substantially similar functionality, or (c) terminate the applicable Subscription Services. In the event of such termination, Saba will refund any subscription fees pre-paid by County for the terminated Subscription Services, pro-rated for the remainder of County's Subscription Term after the effective date of termination.

8.5 The foregoing obligations of Saba shall not apply to any infringement Claim to the extent due to (a) County's use of the Services in a manner other than in accordance with this Agreement; (b) County's use of the Services in conjunction with Content or data where use with such Content or data gave rise to the infringement Claim; and/or (c) County's use of the Service(s) with other software, hardware or services, where use with such other software, hardware or services gave rise to the infringement Claim.

The foregoing states Saba's entire obligation and County's sole and exclusive remedy for any claim of infringement of any third party copyright, trade secret, patent or other proprietary right.

9. Confidentiality. Each party acknowledges that it will have access to certain confidential information of the other party concerning the other party's business, plans, customers, technology, and products, and other information held in confidence by the other party ("Confidential Information"). Confidential Information will include all information in tangible or intangible form that is marked or designated as confidential or that, under the circumstances of its disclosure, should be considered confidential. Confidential Information will also include, but

not be limited to, the non-public portions of the Subscription Services, network design and documentation; any benchmark testing of the Subscription Services; the terms and conditions of this Agreement; and all Content. A party receiving any Confidential Information ("Recipient") of the other party ("Discloser") will use at least the same care to prevent disclosure and unauthorized use of such information as Recipient uses with respect to its own confidential and proprietary information of like importance under similar circumstances, which will not be less than reasonable care. Recipient will not disclose Confidential Information to any third parties, provided that Recipient may disclose the Confidential Information to its employees and contractors who need to know such information and who are bound in writing by restrictions regarding disclosure and use of such Confidential Information comparable to those set forth herein. Recipient will not use any Confidential Information for any purpose other than to exercise its rights and perform its obligations under this Agreement. The foregoing restrictions on disclosure and use will not apply with respect to any Confidential Information to the extent such Confidential Information: (a) was or becomes publicly known through no wrongful act or omission of Recipient; (b) was rightfully known by Recipient before receipt from Discloser; (c) is independently developed by Recipient (i.e., without the use of or reference to the Confidential Information of the Discloser); or (d) becomes rightfully known to Recipient without confidential or proprietary restriction from a source other than Discloser that does not owe a duty of confidentiality to Discloser with respect to such Confidential Information. Recipient may disclose Confidential Information to the extent Recipient is legally required to disclose such Confidential Information, provided, however, that prior to any such required disclosure, Recipient will give Discloser reasonable advance notice of any such disclosure and will cooperate with Discloser in protecting against any such disclosure and/or obtaining a protective order narrowing the scope of such disclosure and/or use of the Confidential Information.

10. Termination.

10.1 Termination for Cause. Either party may terminate this Agreement if the other party materially breaches this Agreement and does not cure such breach within thirty (30) days after receipt of written notice of such breach from the non-breaching party; provided that the cure period for non-payment of the initial Order hereunder shall be ten (10) business days.

10.2 Effect of Termination. Upon the effective date of termination of this Agreement:

- a. Saba will immediately cease providing the Services. On County's request, at any time during the thirty (30) day period following the effective date of termination, Saba will provide to County all Content in the Saba system. County data generated by the Saba system during the Subscription Term will be provided in .csv format, and all other County content or materials stored in the Saba system will be returned in the format in which it was supplied to Saba by County. For the avoidance of doubt, County has the right to retrieve its Content at any time during any Subscription Term. After the expiration of the foregoing thirty (30) day period, Saba will delete all County Content, and will confirm such deletion upon County request;

- b. any and all of County's payment obligations under this Agreement for the Services provided through the effective date of termination will immediately become due; and
- c. In the event of termination for cause by County pursuant to Section 10.1 or termination for Chronic Problems as provided in Exhibit 3, Saba will refund any subscription fees pre-paid by County, pro-rated for the remainder of County's Subscription Term after the effective date of termination.

10.3 Survival. The obligations of the parties under this Agreement, which by their nature would continue beyond termination, cancellation, or expiration of this Agreement, shall survive termination, cancellation, or expiration of this Agreement.

11. Miscellaneous Provisions.

Entire Agreement. This Agreement, including any Order and all documents incorporated herein by reference, constitutes the complete and exclusive agreement between the parties with respect to the subject matter hereof, and supersedes and replaces any and all prior or contemporaneous discussions, negotiations, understandings and agreements, written and oral, regarding such subject matter. County acknowledges that any Orders made hereunder are not reliant, or contingent upon, the delivery, or promise of delivery, of any future functionality, features, products or services. The terms set forth in this Agreement and any Order will control in the event that there are any different or additional terms set forth on any purchase order or other form that County submits. This Agreement may not be modified or amended except in writing signed by a duly authorized representative of each party.

Governing Law. This Agreement is made under and will be governed by and construed in accordance with the laws of the State of California, USA. To the extent not expressly prohibited by any applicable law, the United Nations Convention on Contracts for the International Sale of Goods and all international and domestic legislative or other implementations of such Convention, will not apply to this Agreement.

HIPAA. County expressly agrees that Content shall not include, and Saba shall have no liability for, any Protected Health Information subject to the Health Insurance Portability and Accountability Act ("HIPAA").

Export Laws. Each party shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Subscription Services. Without limiting the foregoing, (i) each party warrants and represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports, and (ii) County shall not permit Users to access or use the Subscription Services in violation of any U.S. or United Nations export embargo, prohibition or restriction.

Severability; Waiver. In the event any provision of this Agreement is held by a tribunal of competent jurisdiction to be contrary to the law, the remaining provisions of this Agreement will remain in full force and effect. The waiver of any breach or default of this Agreement will not constitute a waiver of any subsequent breach or default, and will not act to amend or negate the rights of the waiving party.

Publicity. Promptly after the Effective Date, the parties will cooperate reasonably to issue a mutually acceptable press release announcing County's selection of Saba. Following go-live of the production environment of the Subscription Services ordered hereunder, County agrees that Saba may use County's name in Saba's County lists, and, at Saba's request (i) County agrees to be available as a County reference for reference calls or onsite visits, and/or to present at Saba public events, as approved by mutual agreement of the parties; and (ii) the parties will cooperate reasonably to prepare a mutually acceptable and approved "Success Story/Case Study" about County's use of Saba's products and services, which may be used and made publicly available by Saba for marketing purposes.

Assignment. Neither party may assign this Agreement either in whole or in part without the prior written consent of the other party, except that either party may assign this Agreement to its affiliate or to a successor to all or substantially all of the business or assets of such party (whether direct or indirect, by operation of law or as the result of an acquisition, merger or other such change of control). Saba may also delegate the performance of certain Services to third parties, provided Saba controls the delivery of such Services to County and remains responsible to County for the delivery of such Services. This Agreement will bind and inure to the benefit of each party's successors and permitted assigns.

Notices. Any notice hereunder will be in writing and delivered in person or by courier, sent by email or confirmed facsimile (fax), or mailed by certified or registered mail, postage prepaid, return receipt requested, and addressed as set forth on the Order or to such other address as given in accordance with this Section. If notice is given in person, by courier or by email or fax, it will be effective upon receipt; and if notice is given by mail, it will be effective five (5) business days after deposit in the mail.

Notice to County:	Ric Giardina, Workforce Development Manager County of Sonoma Human Resources Dept. 575 Administration Drive, Suite 117C Santa Rosa, CA 95403 ric.giardina@sonoma-county.org
with a copy to:	Christina Cramer, Director County of Sonoma Human Resources Department Workforce Development Manager County of Sonoma Human Resources Dept. 575 Administration Drive, Suite 116B Santa Rosa, CA 95403 christina.cramer@sonoma-county.org
Notice to Saba:	Vik Mohindra Senior Account Executive 4120 Dublin Boulevard, Suite 200 Dublin, CA 94568 vmohindra@saba.com
with a copy to:	Saba Software, Inc.

	(Attn: Legal Department) 4120 Dublin Boulevard, Suite 200 Dublin, CA 94568 Legal@saba.com
--	--

Remedies. The parties agree in the event of an actual or threatened material breach of this Agreement, the non-breaching party will be entitled to seek immediate injunctive relief, in addition to whatever remedies it might have at law or under this Agreement. Except as otherwise expressly provided herein, all rights and remedies hereunder are cumulative, may be exercised singularly or concurrently and will not be deemed exclusive. If any legal action is brought to enforce any obligations hereunder, the prevailing party will be entitled to receive its attorneys' fees, court costs and other collection expenses, in addition to any other relief it may receive.

Force Majeure. Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control.

This Agreement includes the following Attachments

Attachment 1: Saba Cloud Entitlements

Attachment 2: Saba Customer Privacy Policy

Attachment 3: Saba Information Security Policy

Attachment 4: Saba Disaster Recovery and Business Continuity Policy

Attachment 5: Saba Cloud Support Policy

Attachment 6: Insurance Requirements

Saba Software, Inc.

DocuSigned by:

Phil Saunders

63CD8AE82801491

By: Phil Saunders

Title: President & CEO

Date: February 4, 2019

County of Sonoma

CERTIFICATES OF INSURANCE REVIEWED AND ON FILE:

By: *Christina Cramer*

Christina Cramer, Human Resources Director

Date: 2/1/19

APPROVED AS TO FORM FOR COUNTY:

By: *[Signature]*

County Counsel

2-1-19

Policies and Entitlements

1. [Saba Cloud Policies](#)
2. [Saba Cloud Entitlements](#)
3. [Saba Enterprise Cloud Policies](#)
4. [Saba Enterprise Cloud Entitlements](#)
5. [Pedagogue Policies](#)
6. [Comartis Policies](#)
7. [HumanConcepts Policies](#)
8. [Content Delivery Network Policies](#)
9. [Transition Manager Policies](#)
10. [VEMS Policies](#)

Saba Cloud Policies

- 1 [Customer Privacy Policy](#)
- 2 [Saba Acceptable Use Policy](#)
- 3 [Information Security Policy](#)
- 4 [Disaster Recovery Policy](#)
- 5 [Saba Cloud Support Policy](#)

Saba Cloud Entitlements

- 6 [Saba Cloud Entitlements](#)

Transition Manager and **Saba Planning**: The policies applicable to Saba Cloud apply to these products as well (with the exception of the Support Policy, which is specific to each product)

Saba Enterprise Cloud Policies

7 Saba Enterprise Cloud Support Policy

Customer Privacy Policy (same as above, under Saba Cloud Policies)

Saba Acceptable Use Policy (same as above, under Saba Cloud Policies)

Business Continuity and Disaster Recovery Planning (same as above, under Saba Cloud Policies)

Information Security Policy (same as above, under Saba Cloud Policies)

Saba Enterprise Cloud Entitlements

Enterprise Cloud Edition	Locale (Language Version) Entitlement
Professional Edition	English plus one (1) local locale *
Premium Edition	English plus one (1) local locale *
Dedicated Premium Edition	English plus one (1) local locale *

* Customer may, upon written notice to Saba at any time during the term of a subscription agreement (provided Customer is not in breach of the agreement), and at no additional charge, exchange any of the Saba Locales initially ordered on the Order Date for any other Saba Locale that is generally commercially available provided that a) the replacement Saba Locale is the functional equivalent of the original; and b) the replacement Saba Locale was generally commercially available as of the Order Date; and c) the replacement Saba Locale and the original are available at the same list price as of the replacement date. Following any such exchange Customer shall not have the right to use original language version.

Subscription Service Edition	Locale (Language Version) Entitlement
Business Edition	Three (3) Locales *
Enterprise Edition	Five (5) Locales *

Global Edition	Seven (7) Locales *
----------------	---------------------

* Customer may, upon written notice to Saba at any time during the term of a subscription agreement (provided Customer is not in breach of the agreement), and at no additional charge, exchange any of the Saba Locales initially ordered on the Order Date for any other Saba Locale that is generally commercially available provided that a) the replacement Saba Locale is the functional equivalent of the original; and b) the replacement Saba Locale was generally commercially available as of the Order Date; and c) the replacement Saba Locale and the original are available at the same list price as of the replacement date. Following any such exchange Customer shall not have the right to use original language version.

Saba Enterprise Cloud Entitlements *

Entitlement	Professional Edition	Premium Edition	Dedicated Premium Edition
Domains	1	Unlimited	Unlimited
Content Storage	1 GB	5 GB	10 GB
Development / Staging / QA / Test Environments	0	1	2
Control Over Upgrades	N/A	N/A	Yes **
Authorized Support Contacts	2	4	6
Phone Support Hours	8x5	24x7	24x7

* Entitlements may vary for Testing & Assessment.

** Customer version cannot be more than one version behind current Saba release.

Pedagogue Policies

- 8 Terms for Renewing Pedagogue Customers
- 9 Business Continuity and Disaster Recovery Planning
Information Security Policy **(same as above, under Saba Cloud Policies)**
- 10 Privacy Policy
- 11 Technical Support Policy

Comartis Policies

- 12 Technical Support Policy (English)
Technical Support Policy (German) **(not needed, so not downloaded)**

HumanConcepts Policies

- 13 Subscription Services Support & SLA Policy
- 14 BTF Support Services Terms

Content Delivery Network Policies

- 15 Content Delivery Network Flowdown Terms

Transition Manager Policies

- 16 Transition Manager Support Policy

Validated Environment Managed Services (VEMS)

- 17 VEMS Policy

© 2019 Saba Software, Inc. All rights reserved.

Attachment 2 - Saba Customer Privacy Policy

Saba Hosted Customer Privacy Policy



Last Revised 22 October 2018

1. Introduction

Saba is committed to protecting information which can be used to directly or indirectly identify an individual ("personal data") in the course of its business with its customers ("Customers"). For that reason, Saba created this Policy which explains what personal data Saba collects, the purposes for which it is used and shared, how customers may correct such data, and how Saba safeguards that data.

This Policy is subject to the terms and conditions of your customer agreement with Saba and any Data Protection Agreement (including any standard contractual clauses) you may have entered into with Saba (collectively the "Agreements"). In the event of any conflict or inconsistency between the terms and conditions of this Policy and those of the Agreements, the terms and conditions of the Agreements will prevail.

This Policy applies to: (i) the hosted environments (the "Hosted Environments") where Saba makes its software products available to our customers; and (ii) Saba's processing of Customer personal data in the normal course of administering and otherwise fulfilling our Agreements with Customers ("Administration"). References to "Saba", "we" or "us" means Saba Software, Inc., and its affiliated entities worldwide.

2. APEC Cross Border Privacy Rules & U.S. Privacy Shield Framework

Saba's privacy practices described herein comply with the APEC Cross Border Privacy Rules System. For more information, please visit: <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSCG/CBPR/CBPR-PoliciesRulesGuidelines.ashx>.

Saba Software, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. We are committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List <https://www.privacyshield.gov/>.

Saba is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Saba complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions. With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Saba is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at <https://feedback-form.truste.com/watchdog/request>. Under certain conditions, more fully described on the Privacy Shield website [<https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>], you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

3. Basis for Processing

Saba processes personal data as required to fulfil our Agreements with Customers, in order to comply with applicable laws, rules and regulations and further to Saba's legitimate interests.

As may be required by applicable law, we may also seek your explicit consent to process certain personal data provided by you or collected on a Hosted Environment. Any consent will be entirely voluntarily. However, should you choose not to grant the requested consent to the processing of your personal data, certain offerings or services may limited in scope or not available.

4. Collection of personal data

Hosted Environments.

Saba's Hosted Environments allow our Customers to upload personal data about their staff and prospective staff, including names, addresses, resumes, performance reviews competencies and compensation information. Customers have sole control over the persona data they choose to upload into Saba's Hosted Environments. Saba does not process the personal data uploaded by Customers to the Hosted Environments for any purpose other than as described in our Agreements and this Policy.

Administration.

We may collect personal data that you choose to provide to us. For example, this may occur when you:

- submit orders for products and services;
- register for events, training or other Saba offerings;
- request support, ask us to contact you, or pose questions for us to answer; or
- otherwise provide personal data to Saba.

In such cases, we may collect personal data such as: your first and last name, location, your postal and email address, your telephone number, social media information, and certain information about the company you are working for, such as: your company's name, address, your job title/seniority level. In the event you choose to provide Saba with your social media information, Saba may retrieve publicly available information about you on such social media platforms.

Hosted Environment Usage Information

When you visit our Hosted Environment, we may collect information regarding your visit to better improve our Hosted Environment and your experience with it. More specific details about information we may collect is as follows:

(a) Cookies

We use cookies to simplify your access and to tailor our services to your needs and interests. You can control the use of cookies at the individual browser level. If you reject cookies, you may still use our Hosted Environment, but your ability to use some features or areas of our Hosted Environment may be unavailable or limited. Some of the cookies we use and their functionality are:

- (a) JSession ID – this maintains the session info in Saba Cloud;
- (b) CSession ID – needed for content security and privacy;
- (c) Google Analytics – turned on by request for Customers who use Google Analytics; and
- (d) Remember Me – turned on my request by Customer, to allow auto-login instead of providing ID and password each time.

(b) IP Addresses, Log Files & Other Data

As is true of most web sites, we gather certain information automatically and store it in log files. This information may include internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and/or clickstream data.

5. Use and Purpose of Collected Personal Data

Saba uses personal data to:

- confirm and fill orders for products and services;
- provide contracted services;
- administer accounts;
- maintain databases and subscription lists;
- alert you to service issues, product upgrades, updated information and other new or complimentary products and services;
- provide support and respond to queries;
- otherwise conduct its business operations; and
- contact you as necessary for the above purposes.

Saba may use aggregated and non-personally identifiable information arising from Customer's use of the Hosted Services (but not any personal data or Customer content), without restriction or remuneration. Such use may include, but not be limited to:

(a) providing services to Customer; (b) improving or creating Saba products and services; (c) compiling statistical and performance information related to the Hosted Services, and/or (d) developing and distributing benchmarks and similar reports and databases.

We will not use personal data for any other purpose incompatible with the purposes listed in the Agreements or this Policy, unless it is authorized by you, or is necessary for us to comply with a legal obligation.

6. Sharing Your Personal Data

Personal data may be shared within the companies making up the Saba group, solely in connection with the purposes set out in the Agreements and this Policy. All such companies are bound by appropriate data processing agreements and/or confidentiality undertakings, and will only use personal data in accordance with this Policy. Such companies are located within the European Economic Area, in countries that are regarded by the EU Commission as featuring an adequate level of data protection, or are subject to a valid transfer mechanism.

Personal data may also be shared, as required, with those who provide products and/or services to Saba and its customers - such as web site hosting, information technology consulting, web site management, foreign language support, complementary products and services requested by Users, data analysis, audit, legal, administrative, back-up, security, marketing and promotion. We only provide these third parties with the minimum amount of personal data necessary to provide the services on our behalf, and the third parties are (where legally required) bound by appropriate order data processing agreements and/or comprehensive confidentiality undertakings and therefore not permitted to use your personal data except for the limited purpose of completing the requested service or transaction.

Circumstances may arise where Saba may decide to sell, buy or otherwise reorganize some or all of its business. Such a transaction may involve, in accordance with applicable law, the disclosure of personal data to prospective or actual purchasers. Saba will seek appropriate protection for personal data in these types of transactions. Saba may also retain and disclose personal data in order to: (1) comply with applicable laws; (2) respond to governmental inquiries or requests; (3) comply with valid legal processes; (4) protect the rights, privacy, safety or property of Saba, Hosted Environment visitors, clients or the public; and (5) enforce our Hosted Environment terms of service.

7. Security and Confidentiality

Saba takes appropriate and commercially reasonable technical and organizational measures to protect personal data against unauthorized access, accidental loss or damage and unauthorized destruction, as set out in the Agreements. Saba staff and third parties who handle personal data are required to treat it confidentially and are not permitted to use or share it except as provided in this Policy.

Customers are responsible for the content, including personal data, on their Hosted Environments. Customer will collect and process all personal data contained in their Hosted Environments in compliance with applicable law, including all applicable privacy laws.

8. Data Retention

We will not keep personal data longer than as necessary for the fulfillment of the purposes outlined herein, or as required by law or regulation. We seek to avoid the retention of unnecessary or duplicative information.

9. Access, Deletion and Correction

Hosted Environments:

Customers can themselves access, correct and delete personal data on the Hosted Environments as they see fit.

Administration:

Our goal is to ensure Customer personal data Saba processes outside of the Hosted Environments is accurate and complete. Customers can help us accomplish this by letting us know when it changes. Customers may access, correct, or ask us to delete, your personal data by contacting your account representative.

10. Contact Information

Questions regarding this Policy should be directed to Saba by contacting us at: DataPrivacyRequests@saba.com.

Saba's headquarters office is located at 4120 Dublin Boulevard, Suite 200, Dublin, CA 94568.

11. Updates to Policy

We may update this Policy from time to time. When we do so, changes in our Policy will be effective immediately upon posting the revised Policy to Saba's Policies and Entitlements page at: <https://policy.saba.com/profile/>. As a result, we recommend that you check this Policy on a regular basis.



Saba Cloud: Customer Information Security, Quality & Assurance Policy Statement

Saba Security, Risk & Compliance
Effective: June 2018



Customer Information Security, Quality & Assurance Policy Statement

1. Purpose & Scope

The purpose of this document is to communicate Saba's administrative, physical and technical measures in place to protect the confidentiality, integrity and availability of customer data provided to Saba when using the Saba Cloud platform.

2. Statement of Commitment

As a top business priority, Saba is committed to demonstrating to our customers that we are a trusted supplier that has implemented industry standard information security and privacy processes and controls to ensure the appropriate protection of customer data ("Data"), as further described herein.

3. Corporate Information Security

3.1. Governance & Accountability & Risk Management

To address the effective management of and compliance with Saba's information security and privacy obligations, as well as manage risk, Saba has established the following:

- 3.1.1. A VP & Chief Information Security Officer (CISO) leads a dedicated Security, Risk and Compliance (SRC) function responsible and accountable for information security.
- 3.1.2. An IT Committee and Security Council with cross-functional engagement across multiple corporate functions supporting Saba's products and services with the following objectives:
 - a) Communication of new security risks, vulnerabilities and/or audit and compliance issues requiring corrective action; and
 - b) To maintain awareness of significant business or operational changes that may introduce new risks or impact the effectiveness of policies and controls.
- 3.1.3. A common policy governance framework that is:
 - a) Providing clear and concise communication of directives, conduct expectations and protocols.
 - b) Approved by management and adheres to corporate document quality standards and reviewed on an annual basis.
 - c) Supported by established processes with defined roles and responsibilities, procedural guidance, and/or technical standards.
 - d) Supported by the implementation of controls that are validated by internal and external audits for ongoing effectiveness.
- 3.1.4. Annual third party external, and regular internal audits and risk assessments are conducted to validate continued policy effectiveness and compliance. This includes an exception process to formally document management's risk treatment plan and/or acceptance supported by the business rationale.

3.2. Personnel & Corporate IT Security

To address the integrity and competency of all Saba personnel, Saba has established the following:

- 3.2.1. Human resources and corporate IT on-boarding and off-boarding procedures, with process checklists to support completing the sequential and required steps.
- 3.2.2. All potential hires are subject to background screening, including:
 - a) Baseline verification for all personnel (e.g., criminal, education and employment backgrounds); and
 - b) Extended verification for specific role or functional designations (e.g., credit).

- 3.2.3. Confidentiality agreements must be signed at induction.
- 3.2.4. Personnel role designation (e.g., job title) must be assigned within the appropriate management organizational structure and responsibilities are defined in accordance with job performance expectations that are evaluated by line management. All staff must complete certain mandatory training, including the following:
 - a) Compliance training;
 - b) Security and privacy awareness training; and
 - c) Supplemental procedural or technical training (as applicable).
- 3.2.5. Management authorization must be obtained prior to provisioning (or modifying) physical and logical access commensurate to the role and responsibilities.
- 3.2.6. Prior to issuing user IT computing equipment (e.g., laptops) the following must be completed by IT personnel:
 - a) Uniquely identifiable asset tags applied to the equipment which has been recorded in the corporate IT asset inventory;
 - b) Corporate network user access is provisioned following the standard credential account creation processes and naming conventions; and
 - c) Baseline security applications are installed and appropriately configured for endpoint protection.
- 3.2.7. Logical and physical access are withdrawn and user IT computing equipment is returned in a timely manner when staff leave Saba.

3.3. User & Network Access Control

To address the control of logical access to Saba applications and systems that process Data, the following are in place:

- 3.3.1. User access provisioning is controlled by the following:
 - a) Users are uniquely authenticated and the use of shared accounts restricted;
 - b) Industry standard password strength and complexity is enforced and passwords remain encrypted using industry standard secure hashes; and
 - c) User access is authorized and provisioned with the least privilege necessary as appropriate for role designation
- 3.3.2. Administrative and/or elevated privileged user access and user activity is monitored with the following:
 - a) Audit logs of system events, which are reviewed and securely retained; and
 - b) Use of Intrusion detection/prevention systems (IDS/IPS) and log management and/or security information and event management (SIEM) systems
- 3.3.3. User access is controlled with the following:
 - a) Use of network perimeter firewalls that control and protect network traffic between internal (private) and external public (Internet) or untrusted networks;
 - b) Use of virtual private networking (VPN) for remote access and multi-factor authentication (MFA) for production applications and systems; and
 - c) Wireless network access connections are authenticated based on industry standard encryption protocols and only permitted in office buildings and/or designated workplaces



3.4. Physical Access & Environmental Security

To address the control of physical access and environmental protection for facilities that house Saba applications and systems that process Data, the following are in place:

- 3.4.1. Access to such facilities is controlled using proximity badge reader security systems with ingress/egress activity logging enabled;
- 3.4.2. All personnel maintain visible photo-identifiable badges;
- 3.4.3. Access to data centers, server rooms or other secure areas is controlled using proximity badge reader security systems, biometrics, PIN codes and/or other higher assurance security measures;
- 3.4.4. Temporary access procedures are established for visitors, guests or external persons upon arriving and departing such facilities, including:
 - a) Registration and sign-in via log register or kiosk;
 - b) Visible temporary badges; and
 - c) Escorted access for entry and while on premise
- 3.4.5. Building main entrance doors remain locked outside regular business hours;
- 3.4.6. Key points of entry and secure areas have defined security perimeters, appropriate barriers, and security cameras.
- 3.4.7. Environmental protections are used for production data centers or server rooms including:
 - a) Surge protection, uninterruptible power supply (UPS) systems, and generator backup power for production datacenter hosting facilities;
 - b) Automatic fire detection alarm and suppression systems suitable for computing equipment and the storage of combustible materials strictly prohibited; and
 - c) Ventilation and cooling to sustain the ambient temperature at levels to prevent damage to computing processing
- 3.4.8. Appropriate supplier due diligence of data center hosting/co-location service providers (pre- and post-contract) is to be completed, and each location has appropriate external third party assurance documentation (e.g., ISO 27001 certification and/or SOC1/SOC2 audit reports).

3.5. Secure Data Processing & Governance

To address Data is appropriately secured and controlled, the following are in place:

- 3.5.1. The customer and Saba acknowledge the customer is the data controller and Saba is the data processor of any Data.
- 3.5.2. Data processing activities adheres to the contractual agreement with the data controller and only commences upon completion of the customer service order.
- 3.5.3. Data processing requests from customers and/or their users must be in writing and systematically recorded.
- 3.5.4. Third party Data transfers must be previously authorized and systematically recorded.
- 3.5.5. Data modification operations (e.g., entering, altering or deletion of data) is pre-authorized by the data controller and procedures are established to return altered data to its original unaltered state.
- 3.5.6. User activity audit logging is enabled and securely retained to trace back individual user Data modification operations (e.g., data entry, alteration or removal and/or deletion).

3.5.7. Appropriate due diligence is completed for sub-processors of Data.

3.5.8. Industry-standard cryptographic methods, protocols and key lengths are used for storing and/or transmitting Data with the following:

- a) 256-bit symmetric key encryption for data storage
- b) TLS 1.2 (Transmission Layer Security) for web servers
- c) SFTP (Secure File Transport Protocol) for file transfers
- d) Secure hashes for encrypted password storage

3.5.9. The secure disposal of Data includes any of the following:

- a) Sanitization, destruction or purging of Data
- b) Secure erasure by cryptographic means, degaussing or physical destruction of hardware or media
- c) Use of shredders or labeled secure disposal bins

3.6. Security Incident Response & Breach Notification

To address awareness and handling of security incidents and notifications, the following are in place:

3.6.1. Timely response to security events and/or incidents that have been reported are handled by Saba's Security Incident Response Team (SIRT) in accordance with the established incident management process. This process includes the following:

- a) Defined roles and responsibilities associated with timely response coordination and security incident (and/or breach) notification protocols including notifying impacted customer(s) without undue delay;
- b) The appropriate methods, tooling and/or partnerships with 3rd party experts required for investigative forensic analysis and chain of custody preservation;
- c) Detection, containment, eradication and recovery procedures and prioritization based on classification and severity of incident; and
- d) Post-incident debrief reporting of cause, impact and lessons learned for incident response planning

4. Product

4.1. Application & Architecture Security

To address that production applications and systems that process Data are protected against security vulnerability threats and/or unauthorized access, the following are in place:

- 4.1.1. Logical and physical production access is restricted to authorized operations personnel.
- 4.1.2. Shared and/or native system accounts and elevated privileged access is strictly limited as necessary. Each such instance is supported by a documented business justification, the list of personnel requiring access and authorization from management.
- 4.1.3. User access to source code is appropriately restricted to authorized engineering personnel.
- 4.1.4. There is separation of duties between operations and engineering personnel, in order to appropriately segment and restrict user access to production data and systems.
- 4.1.5. Physical and/or logical segregation separates production from non-production Data resident in applications, systems and datacenter hosting facilities.
- 4.1.6. The use of removable/portable media devices (e.g. external USB/thumb drives) is strictly prohibited while accessing or using applications and systems processing Data.



4.1.7. Asset and capacity management processes include ongoing maintenance of asset inventories and architecture diagrams and topographies and interconnectivity of systems.

4.1.8. Engineering and operations procedures are established including (but not limited to) the following:

- a) Secure hardening standards and patch management processes are based on industry standards (e.g., NIST, ISO, CIS, etc.);
- b) System administrator and/or operator user manuals;

4.1.9. Security vulnerability assessments are conducted in accordance with industry standards (e.g., NIST, OWASP, CVSS, etc.) and remedial corrective action is prioritized by risk severity using the following multi-pronged tactics and tooling:

- a) Application security penetration testing is conducted by reputable external third party assessors;
- b) Vulnerability scanning is conducted on infrastructure systems (i.e., servers, networking components and databases) on a regular basis using reputable industry accepted tools; and
- c) Application security scans are run during the software development lifecycle (SDLC) process using dynamic and static application security testing (DAST/SAST) tools

4.2. Change Control & Quality Management

To address that production applications and systems processing Data are designed and operate in accordance with defined expectations, the following are in place:

- 4.2.1. Procedures are established, and appropriate tooling is in use, for application development, quality assurance (QA) and system validation testing, and release management processes; and
- 4.2.2. Configuration and system changes are appropriately validated with quality management sign-off prior to and post deployment, in accordance with the established change control process.

4.3. Service Availability

To address business continuity and ensure that products and services are resilient to service disruptions, accident or natural disasters, the following are in place:

- 4.3.1. Policies and procedures are established, which include the following:
 - a) Required use of primary and secondary production data center hosting facilities that do not share common known disaster zones;

- b) Disaster recovery planning with defined recovery objectives (RTO/RPO), that are tested on an annual basis;
- c) Data backup processes are established that include defined frequency of scheduled full and incremental backups, backup storage medium and physical location, and retention period;
- d) Data recovery processes are established and are tested on a periodic basis; and
- e) Service outages are monitored against established customer service level agreements (SLAs).

4.3.2. System redundancies designed in the infrastructure architecture, including:

- a) Multiple telecommunication or internet service providers (ISPs);
- b) Network topologies designed with load balancers and redundant switches, firewalls, and other networking components; and
- c) Disk drives and power supplies that are hot-swappable and mirroring (RAID) for infrastructure components

5. Customer Assurance

5.1. Saba's Security Documentation

5.1.1. Saba has obtained third-party certifications and audits, collectively referred to as Saba's "**Security Documentation**". Upon advance written request at reasonable intervals and subject to confidentiality agreements in place, the following confidential documentation can be made available for customers to review:

- a) Saba's SOC 2 Type 2 annual audit report
- b) SOC 1/SOC 2 audit reports and ISO 27001 certifications for Saba's primary/secondary regional data center hosting facilities

6. Policy Updates

Changes to this document will be posted on Saba's web site at policy.saba.com (or at such other URL(s) as may be designated by Saba from time to time), and those changes will be effective immediately upon posting. We recommend that our customers review this document on a regular basis. By continuing to use Saba's products or services after a revised version of this document has been posted, you will be deemed to have agreed to the changes to this document.



Saba Cloud: Business Continuity & Disaster Recovery Planning Policy

Customer Entitlement Policy



Customer Entitlement Policy > Saba Cloud > Business Continuity & Disaster Recovery Planning Policy

1. Purpose

This document describes Saba's business continuity and disaster recovery (DR) planning policy for customer entitlements associated with the Saba Cloud subscription offering.

2. Introduction

Saba believes that its subscription customers are entitled to smooth, uninterrupted access to the services provided by Saba. Saba places a priority on ensuring service availability, even in the aftermath of a disaster or other unexpected event. This document describes the processes and procedures that Saba has put into place in order to minimize the effects of a potentially disruptive event, and to restore subscription service availability in the aftermath of such an event.

3. Business Continuity

3.1. Saba Offices

Saba maintains a global business presence, with offices and operations on four continents. Key personnel and equipment for business continuity and disaster recovery are distributed across several offices. In the event that one facility is unavailable or taken offline, staff in other locations are in position to repair and restore service delivery. Saba's business continuity planning team has identified crucial systems, hardware and third party applications, together with replacement and restoration parameters. In the event that a natural disaster or man-made event affects any of Saba's services or business facilities, individual employees are tasked with specific, prioritized business continuity responsibilities.

3.2. Datacenter Site Locations

Saba's subscription services are hosted by distributed datacenters that support all Saba regional customers, e.g., United States, Canada, EMEA, and APAC. The regional locations for each Saba datacenter facility is listed in the following table.

Region	Saba Datacenter Locations
United States	<ul style="list-style-type: none"> Watertown, MA Rancho Cordova, CA
Canada	<ul style="list-style-type: none"> Mississauga, Ontario
EMEA	<ul style="list-style-type: none"> Amsterdam, NE London, UK
APAC	<ul style="list-style-type: none"> Sydney, AU Melbourne, AU

3.3. Datacenter Assurance

Saba datacenters are supported 24/7/365 with security personnel and technical support engineers. Environmental controls such as fire, cooling and power systems are fully redundant, and scaled to accommodate component failure. Internet connectivity is assured with not less than three Tier I backbone carriers per datacenter. All datacenters are equipped with redundant and high-density power systems, with automated and monitored facility controls. Power generators at all datacenters are tested regularly and supported by multiple fuel suppliers to ensure continuous operations in the event of a disaster.

All datacenters are selected based on industry standard parameters, including (i) physical location outside the disaster zone for the primary datacenter; (ii) datacenter site compliance based on ISO/IEC 27001 and the AICPA SOC 1 (SSAE 16) and/or SOC 2 (AT-101) Type 2 audit standard; (iii) proximity to a major airport or major IT equipment parts warehouse or distribution center; and/or (iv) practice of carrier neutrality or presence of physically segregated internet connections.

4. Disaster Recovery

4.1. Disaster Recovery Strategy

Saba's Disaster Recovery (DR) strategy is based on daily customer data replication and/or virtual machine file synchronization. Saba maintains dedicated datacenter sites within each region for disaster recovery of Saba's applications for client sites.

In the event that any Saba datacenter is no longer able to service our customers, Saba's disaster recovery plans call for the restoration of operational services, using our recovery datacenters.

In the event that customer data recovery is required as a result of a datacenter outage, Saba will work with each customer to determine the critical information needed, and to agree upon the appropriate time frame to perform the complete restoration. For disaster recovery scenarios, Saba supports a Recovery Point Objective (RPO) of 24 hours with a Recovery Time Objective (RTO) of 72 hours.

4.2. Disaster Recovery Testing

Saba is committed to meeting the business needs of its subscription and hosted customers, even in the event of a disaster or emergency. To ensure that Saba is appropriately prepared to respond to an unexpected event, on an annual basis, Saba tests its disaster recovery processes and procedures. Saba uses the results of this testing process to evaluate its preparedness for disasters and to validate the completeness and accuracy of its policies and procedures. Saba's disaster recovery (DR) planning procedures and test results are validated by an accredited external audit firm and incorporated in Saba's annual SOC 2 Type 2 audit report.

5. Policy Updates

Changes to this document may be posted on Saba's web site at policy.saba.com (or at such other URL(s) as may be designated by Saba from time to time), and those changes will be effective immediately upon posting. We recommend that our customers review this document on a regular basis. By continuing to use the subscription services after a revised version of this document has been posted, you will be deemed to have agreed to the changes to this document.

Attachment 5 - Saba Cloud Support Policy

Policy Document

Customer Support Policy: Saba Cloud

June 2018



Customer Support Policy: Saba Cloud

Overview

This document describes Saba's support policy for its Cloud products and services.

Saba Customer Support Mission

Our number one corporate value is customer success. All of our support processes are designed to ensure that our customers are successful in using our products and services. To ensure customer success, our support services are designed to:

- Resolve issues quickly, effectively, and accurately, in partnership with our customers
- Provide courteous and professional service
- Champion change within Saba to improve our products and services on behalf of the customer
- Help ensure that our customers achieve effective use and optimum value from our products and services
- Be uniquely responsive to urgent situations and customer emergencies
- Achieve a team spirit that is projected in each interaction with our customers

Where to Get Answers

Saba Support Services are offered remotely through various channels as described below.

Self-Service

Customer Community — The Saba Online Community is a space for exchanging advice and best practices, and generating group learning and innovation. It is a rapidly growing community and provides the most up-to-date information and news from across Saba customers, partners, and employees. You can join the Saba Online Community by going to Saba's corporate website at www.saba.com and clicking on the Community tab.

Knowledge Base and Documentation — The Saba Support Portal offers a knowledge base that is a searchable repository of frequently asked questions and other information regarding use of Saba's products and services.

The online knowledge base, along with our product documentation, provides 24x7x365 access to the expertise gained from experience using the Saba product line, and contains the latest and most consistent information about our products and services. It is a dynamic repository and is constantly growing.

Contacting Support and Logging Cases

Upon provisioning of your Saba Cloud environment, you will be introduced to your Support resources via our Onboarding Process.

Support Portal

In the event you are unable to find answers to your queries in our Customer Community and knowledge base, you can submit a case via Saba's Support Portal. The Saba Support Portal (found at support.saba.com) enables customers to chat with Saba Support, create cases, obtain updates, and provide information about cases being worked on by Saba Support.

By Telephone

Telephonic support is available 24 hours a day, 7 days a week. Cases may be opened by calling Saba Customer Support using the numbers below.

AMERICAS

Within the United States toll-free: 877-799-SABA (7222)
Outside the United States: 1-650-581-2575

EMEA

International toll-free: 00 800 CALL SABA (00 800 2255 7222)
Alternate: +44-1344-382999

ASIA/PACIFIC

+612-8622-7598
Australia: 1-800-236872



Authorized Support Contacts

In order to provide the most efficient Support possible, customers are required to establish Authorized Support Contacts (ASC's) for engaging with Saba Support. The ASC's are expected to provide first-level support to all end users of their local instance of the Saba Product. Only the ASC's should interface with Saba Support, via the methods described in this document, for next-level Support as needed.

Customers are allowed four (4) ASC's who shall receive the training specified in Appendix C, and may contact Saba Support in accordance with this Support Policy. Access to support is dependent upon maintaining a current subscription.

Additional ASC's may be added for an additional charge provided they also meet the training requirements as reflected in Appendix C (note: the training certification is free of charge). Please contact your Account Manager for pricing for additional ASC's. You may change any authorized support contact upon advanced written notice to Saba. The new support contact must satisfy the aforementioned minimum training requirements in order to be an authorized contact and be able to submit cases. For continuity purposes, Saba requests that customers retain the same ASC(s) for at least 90 days. There is no limit to the number of portal contacts who may access the self-service resources.

Escalation

Saba Support is committed to making sure you receive the fastest and most effective support experience possible. However, we do recognize that on rare occasions, customers may have the need for a higher level of attention to address an issue. To meet that need, the following simple escalation process is in place to raise the visibility of an issue within Saba.

In order to request escalated priority/visibility for a specific issue, please contact our toll-free Support hotline (numbers listed above in this document) to speak directly to a Support Engineer and request the escalation. It is also a best practice to log a note in the case detailing the reason for escalation and business impact of the issue, if not already done.

Enhancement Requests

Customers may request enhancements through the Customer Community. Customers can sign up to be a member of the community by visiting www.saba.com, clicking the Community tab, and selecting the "sign up" option on the Community login screen.

Enhancements submitted through the Customer Community are monitored by Saba Product Management. Customers also have the ability to vote and comment on requests submitted by other members of the Community.

For full details on the enhancement process, search for "enhancement requests" on your Community home page, and you will find the Community Workspace for enhancements.

Support Service Levels

Details on Support Case Severities and Service Levels are included in the Appendices A and B, attached in this document.

System Maintenance and Outage Communications

Saba makes reasonable efforts to deliver timely communications to inform you of any situations that might involve system downtime on Production (PROD) environments. These are delivered via email alerts, sent to the Authorized Support Contacts in the support system, or, to a designated customer email alias, and are delivered for full PROD outages only. The alerts are intended to communicate the following:

- Advanced notice of planned maintenances
- Commencement, and subsequent completion of, planned maintenance activities
- The commencement, and subsequent completion of, unplanned maintenance activities, including urgent maintenance activities to take corrective action to avoid an outage, or, for urgent activities due to an outage

Appendix A: Saba Cloud SLAs

See Appendix B below for definitions of Case Severity Levels and what case types fit under each.

Case Severity		Response SLA	Resolution SLA
S1	Outage (Prod Environment Only)	30 Min	43 Minutes (99.9% monthly uptime guarantee) cumulative downtime per month.
S2	Module Down (Prod Environment Only)	1 hour	12 hours
S3	Major (Any Environment)	2 Hours	Case update provided every 3 business days until a diagnosis and resolution is available.
S4	Minor (Any Environment)	2 Hours	Case update provided every 3 business days until a diagnosis and resolution is available.
SR	Service Request	2 Hours	Within 48 hours, a time frame will be provided for when the service request will be completed.

Appendix B: Case Severity Levels and Service Request Estimates

Case Severity		Case Types	System	Explanation
S1	Outage (PROD)	Production Down*	PROD	All users unable to log in, all services are unavailable
		SSO Down*	PROD	All users unable to log in via SSO
		Content Down*	PROD	No content can be launched

(Continued on the next page)

Case Severity		Case Types	System	Explanation
S2	Module Down (PROD)	3 rd Party Content Provider Down	PROD	Connection with a specific 3 rd party content provider is down. None of the content provided by the 3 rd party content provider can be launched (eg. OpenSesame content is down).
		Analytics Unavailable	PROD	No Analytics reports can be run, Analytics interface does not load or Analytics subscriptions are not running
		API Down	PROD	All API calls are failing
		Assessment Module Unavailable	PROD	Testing & Assessment service is unavailable
		Cannot Upload Any Content	PROD	Unable to upload any Content.
		Data Extract failing	PROD	All data extracts are failing
		Data Import failing	PROD	All data imports are failing
		Performance degradation	PROD	Significant and consistent performance degradation across the system. Most pages take more than 30 seconds to load
		Prescriptive Rule/Notifications Down	PROD	No Prescriptive Rules are running
		Notifications not sending	PROD	No notification emails are being sent
		Saba Meeting Down	PROD	Saba Meeting is down and cannot be accessed.
		Saba Video	PROD	Saba Video is down. None of the Saba Videos can be launched or viewed.
		Search Functionality Down	PROD	Global search is not working, nothing is returned or an error appears
		SFTP Connection Failure	PROD	SFTP connectivity is down or connections are being refused
S3	Major	Non-Production System Down	Non-Prod	Non-Production system is completely unavailable
		Functionality Troubleshooting	All environments	Any case which requires Saba's help to troubleshoot, for example: <ul style="list-style-type: none"> - Functionality not working as expected or documented - Encountering errors when using functionality - Content is not working as expected - Individual report or API not returning expected data or not running

Policy Document > Saba Cloud

		Intermittent issue	All environments	Particular area of the service (example: Analytics, Integrations, Indexes etc) encountering intermittent and ongoing problems
--	--	--------------------	------------------	---

Case Severity		Case Types	System	Explanation
S4	Minor	How-To	All environments	Example: requesting information on a particular feature or functionality
		Usability	All environments	Example: cosmetic impact
		Contact Management	All environments	Adding or removing Authorized Support Contacts or KB users
		Account Management	All environments	Usage reports, license questions etc
SR	Service Request**	SSO Configuration	All environments	A request to configure SSO, or renew the SSO certificate
		Enable Feature	All Environments	A request to enable or disable a feature
		Refresh request	All Environments	A request to copy Production to non-production system
		Database Extract Deployment	All Environments	A request to deploy a database extract. Customer must have purchased the Premium Data Extract
		SFTP Configuration	All Environments	A request to create a new SFTP account, or whitelist a new IP address for SFTP connectivity
		PGP Configuration	All Environments	A request to configure encryption for SFTP
		Configuration Changes	All Environments	A request to change configuration which can only be completed by the Saba Administrator

*Upon request, a Root Cause Analysis (RCA) can be provided for this case type. RCA's will be provided in a standard Saba template. While each case may have extenuating circumstances causing delays, the general target turnaround time for RCA's is 72 hours following resolution of the issue.

**Saba anticipates that customers will make reasonable use of the Service Request process. Saba reserves the right to decline service requests of a frequency or nature that exceeds the normal business requirements of Saba customers.

***For full system refreshes, 14 days' notice is required and no refresh requests will be processed during the Release Preview period.

Appendix C: Authorized Support Contact Training

Minimum Training Requirements for Certification of Authorized Support Contacts

In order to maximize the benefit of the services provided by Saba Support and to help speed case resolution, authorized support contacts are required to complete an ASC Certification. The certification will supply all new ASCs with documentation and guides which provide a comprehensive resource library of configuration and step-by-step instructions. Training on the tool used to raise tickets is also provided, in a simple "How-to" guide that can be easily referenced should you need to raise a request to Saba's Customer Care team. In addition to the guides, all ASC's can attend any of the free Customer Training offered by Saba Education. A calendar of training events can be located in the Customer Community.

The required certification can be found on the Customer Community. ASC's should first register in the Customer Community; once logged on, they can follow these five simple steps to locate and complete the ASC Certification.

1. From the home page, enter "ASC certification" in the search box.
2. Select the appropriate ASC certification for your Saba product (example, ASC Saba Cloud, SEC 5.5, ASC, SEC 6.x, ASC SEC 7.x)
3. Register for the certification you selected.
4. Launch each activity, for example, launching Documentation and Guides will open a zip file that contains all user guides for that product and version. These guides will help ASC's learn about a specific function, learn about the available options and how to configure, set up and use that function.
5. Complete the acknowledgement.

Additional Training

If you want specific training by role or function, for example, Learning Administrator training or People Administrator training, you can access free Readiness Training. These curricula will provide you with basic training via recorded sessions from Saba education that cover the most frequent actions for different roles. Check back regularly, as more curricula are added every month. To locate the list of available curricula, follow these simple instructions:

1. Log on to the Customer Community.
2. Click Browse.
3. Click Learning Catalog.
4. From the available categories on the left, select the either Saba Cloud Training or Saba Enterprise Training.
5. You can search for "Implementation Readiness Training" or, refine the results by clicking Curriculum under Learning Event Type then clicking Apply Filter.



Saba delivers a cloud-based Intelligent Talent Management™ solution used by leading organizations worldwide to hire, develop, engage, and inspire their people. Intelligent Talent Management uses machine learning to offer proactive, personalized recommendations on candidates, connections, and content to help your employees and organization lead and succeed.

© 2018 Saba Software, Inc. All rights reserved. Saba, the Saba logo, and the marks relating to Saba products and services referenced herein are either trademarks or registered trademarks of Saba Software, Inc. or its affiliates. All other trademarks are the property of their respective owners.

ATTACHMENT 6

INSURANCE REQUIREMENTS

With respect to performance of work under this Agreement, Consultant shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described below unless such insurance has been expressly waived by the attachment of a Waiver of Insurance Requirements. Any requirement for insurance to be maintained after completion of the work shall survive this Agreement.

County reserves the right to review any and all of the required insurance policies and/or endorsements, but has no obligation to do so. Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve Consultant from, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

1. Workers Compensation and Employers Liability Insurance
 - a. Required if Consultant has employees as defined by the Labor Code of the State of California.
 - b. Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.
 - c. Employers Liability with minimum limits of \$1,000,000 per Accident; \$1,000,000 Disease per employee; \$1,000,000 Disease per policy.
 - d. Required Evidence of Insurance: Certificate of Insurance.

If Consultant currently has no employees as defined by the Labor Code of the State of California, Consultant agrees to obtain the above-specified Workers Compensation and Employers Liability insurance should employees be engaged during the term of this Agreement or any extensions of the term.

2. General Liability Insurance
 - a. Commercial General Liability Insurance on a standard occurrence form, no less broad than Insurance Services Office (ISO) form CG 00 01.
 - b. Minimum Limits: \$1,000,000 per Occurrence; \$2,000,000 General Aggregate; \$2,000,000 Products/Completed Operations Aggregate. The required limits may be provided by a combination of General Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance. If Consultant maintains higher limits than the specified minimum limits, County requires and shall be entitled to coverage for the higher limits maintained by

Consultant.

c. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds \$25,000 it must be approved in advance by County. Consultant is responsible for any deductible or self-insured retention and shall fund it upon County's written request, regardless of whether Consultant has a claim against the insurance or is named as a party in any action involving the County.

d. [insert exact name of additional insured] shall be endorsed as additional insureds for

liability arising out of operations by or on behalf of the Consultant in the performance of this Agreement.

e. The insurance provided to the additional insureds shall be primary to, and non-contributory with, any insurance or self-insurance program maintained by them.

f. The policy definition of "insured contract" shall include assumptions of liability arising out of both ongoing operations and the products-completed operations hazard (broad form contractual liability coverage including the "f" definition of insured contract in ISO form CG 00 01, or equivalent).

g. The policy shall cover inter-insured suits between the additional insureds and Consultant and include a "separation of insureds" or "severability" clause which treats each insured separately.

h. Required Evidence of Insurance:

i. Copy of the additional insured endorsement or policy language granting additional insured status; and

ii. Certificate of Insurance.

3. Automobile Liability Insurance

a. Minimum Limit: \$1,000,000 combined single limit per accident. The required limits may be provided by a combination of Automobile Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance.

b. Insurance shall cover all owned autos. If Consultant currently owns no autos, Consultant agrees to obtain such insurance should any autos be acquired during the term of this Agreement or any extensions of the term.

c. Insurance shall cover hired and non-owned autos.

d. Required Evidence of Insurance: Certificate of Insurance.

4. Professional Liability/Errors and Omissions Insurance

a. Minimum Limits: \$1,000,000 per claim or per occurrence; \$1,000,000 annual aggregate.

b. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds \$25,000 it must be approved in advance by County.

c. If Consultant's services include: (1) programming, customization, or maintenance of software; or (2) access to individuals' private, personally identifiable information, the insurance shall cover:

i. Breach of privacy; breach of data; programming errors, failure of work to meet contracted standards, and unauthorized access; and

ii. Claims against Consultant arising from the negligence of Consultant, Consultant's employees and Consultant's subcontractors.

d. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

e. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

f. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the

claims-made retroactive date.

5. Standards for Insurance Companies

Insurers, other than the California State Compensation Insurance Fund, shall have an A.M. Best's rating of at least A:VII.

6. Documentation

a. The Certificate of Insurance must include the following reference: [insert contract number or project name].

b. All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. Consultant agrees to maintain current Evidence of Insurance on file with County for the entire term of this Agreement and any additional periods if specified in Sections 1 – 4 above.

c. The name and address for Additional Insured endorsements and Certificates of Insurance is: [insert exact name and address].

d. Required Evidence of Insurance shall be submitted for any renewal or replacement of a policy that already exists, at least ten (10) days before expiration or other termination of the existing policy.

e. Consultant shall provide immediate written notice if: (1) any of the required insurance policies is terminated; (2) the limits of any of the required policies are reduced; or (3) the deductible or self-insured retention is increased.

f. Upon written request, certified copies of required insurance policies must be provided within thirty (30) days.

7. Policy Obligations

Consultant's indemnity and other obligations shall not be limited by the foregoing insurance requirements.

8. Material Breach

If Consultant fails to maintain insurance which is required pursuant to this Agreement, it shall be deemed a material breach of this Agreement. County, at its sole option, may terminate this Agreement and obtain damages from Consultant resulting from said breach, pursuant to Section 10 of the Agreement. These remedies shall be in addition to any other remedies available to County.