STANDARD CONTRACT FOR AWS MARKETPLACE

1. Scope.

1.1 Terms and Conditions. This Standard Contract for AWS Marketplace (the "**Standard Contract**") sets forth the terms and conditions applicable to the licensing of Product from the licensor ("**Licensor**") by the Party (defined below) subscribing to the Product ("**Buyer**"), whether deployed into Buyer's Computing Environment and/or made available as SaaS Service from Licensor's Computing Environment. This Standard Contract only applies if the Product is expressly offered pursuant to the Standard Contract. The offer of Product pursuant to this Standard Contract, and Buyer's purchase of the corresponding Subscription, constitutes each Party's respective acceptance of this Standard Contract and their entry into this Agreement (defined below), and this Agreement will become effective on the date of Buyer's purchase of the corresponding Subscription. Unless defined elsewhere in this Standard Contract, terms in initial capital letters have the meanings set forth in Section 13. Buyer and Licensor may be referred to collectively as the "**Parties**" or individually as a "**Party**".

1.2 Product Subscription. Licensor will fulfill the Subscription to Buyer. A Subscription, as described in the applicable Product Listing and the corresponding purchase transaction, may be for Product deployed in Buyer's Computing Environment and/or Product deployed via SaaS Service through Licensor's Computing Environment. The pricing and term of the Subscription (if not on demand) are set forth in the Product Listing. Additional information concerning the Product and included services that are included or referenced in the Product Listing are a part of the Product Listing; such information may include but is not limited to: intended geographic use of the Product, any technical requirements for use of the Product, Support Services (which may vary by geography), information regarding Open Source Software and a description of Licensor's security practices.

1.3 Agreement. Each Subscription is subject to and governed by this Standard Contract, the applicable Product Listing, the terms and conditions of the NDA (if any and as defined in Section 6.4), the Privacy and Security Terms for SaaS Service Subscriptions, and any amendments to any of the foregoing as may be agreed upon by the Parties in accordance with Section 12.3, which together constitute the entire agreement between Buyer and Licensor (the "**Agreement**"). Each Subscription is a separate agreement between Buyer and Licensor. In the event of any conflict between the terms and conditions of the various components of this Agreement, the following order of precedence will apply: (a) any amendment agreed upon by the Parties; (b) the Privacy and Security Terms for SaaS Service Subscriptions; (c) the NDA (if any); (d) the Product Listing; and (e) this Standard Contract.

2. Licenses.

2.1 Licensed Materials.

2.1.1 If the Subscription is for a Product, or includes a component of a Product,

deployed in Buyer's Computing Environment, Licensor hereby grants to Buyer during the term of the Subscription, subject to Section 2.1.3, a nonexclusive, worldwide (subject to Section 12.4), nontransferable (except in connection with an assignment permitted under Section 12.2), nonterminable (except as provided in Section 10) license under all Proprietary Rights in and to the Product, or the applicable Product component, to deploy, operate and use the Product in Buyer's

Computing Environment and to allow its Users to access and use the Product, or the applicable Product component, as so deployed, in accordance with the Product Listing, the usage purchased in the Subscription, and the terms and conditions of the Agreement.

2.1.2 If the Subscription is for a Product, or includes a Product component,

deployed via SaaS Service, Licensor hereby grants to Buyer during the term of the Subscription, subject to Section 2.1.3, a nonexclusive, worldwide (subject to Section 12.4), nontransferable (except in connection with an assignment permitted under Section 12.2), non-terminable (except as provided in Section 10) license under all Proprietary Rights in and to the Product, or the applicable Product component, to access and use the Product via the SaaS Service and to allow its Users to access and use the Product, or the applicable Product component, and SaaS Service, in accordance with the Product Listing, the usage purchased in the Subscription, and the terms and conditions of the Agreement.

2.1.3 Regardless of whether Buyer deploys the Product in Buyer's Computing Environment or accesses the Product via the SaaS Service, Buyer may use the Product only: (a) in support of the internal operations of Buyer's and its Affiliates' business(es) or organization(s); (b) in connection with Buyer's and its Affiliates' products and services (but, for clarity, not as a stand-alone product or service of Buyer or its Affiliates); and/or (c) in connection with Buyer's and its Affiliate's interactions with Users.

2.1.4 Buyer may make a reasonable number of copies of the Documentation as

necessary to use such Product in accordance with the rights granted under this Agreement, provided that Buyer includes all proprietary legends and other notices on all copies. Licensor retains all rights not expressly granted to Buyer under this Agreement.

2.2 Affiliates and Contractors. With respect to Affiliates and Contractors that Buyer allows to use the Licensed Materials: (a) Buyer remains responsible for all obligations hereunder arising in connection with such Affiliate's or Contractor's use of the Licensed Materials; and (b) Buyer agrees to be directly liable for any act or omission by such Affiliate or Contractor to the same degree as if the act or omission were performed by Buyer such that a breach by an Affiliate or a Contractor of the provisions of this Agreement will be deemed to be a breach by Buyer. The performance of any act or omission under this Agreement by an Affiliate or a Contractor for, by or through Buyer will be deemed the act or omission of Buyer.

2.3 Restrictions. Except as specifically provided in this Agreement, Buyer and any other User of any Licensed Materials, in whole or in part, may not: (a) copy the Licensed Materials, in whole or in part; (b) distribute copies of Licensed Materials, in whole or in part, to any third party; (c) modify, adapt, translate, make alterations to or make derivative works based on Licensed Materials or any part thereof; (d) except as permitted by Law, decompile, reverse engineer, disassemble or otherwise attempt to derive source code, algorithms or the underlying structure of the Product; (e) use, rent, loan, sub-license, lease, distribute or attempt to grant other rights to any part of the Licensed Materials to third parties; (f) use the Licensed Materials to act as a consultant, service bureau or application service provider; or (g) permit access of any kind to the Licensed Materials to any third party.

2.4 Open Source Software. Subject to the requirements of Section 5.1(d), Product may contain or be provided with Open Source Software. If Buyer's use of the Product subjects Buyer to the terms of any license governing the use of Open Source Software, then information identifying such Open Source Software and the applicable license shall be incorporated or referenced in the Product Listing or Documentation. The terms of this Agreement apply to Open Source Software (i) to the extent not prohibited by the license to which the Open Source Software is subject, including without limitation, warranties and indemnification, and (ii) except to the extent required by the license to which the Open Source Software is subject, in which case the terms of such license will apply in lieu of the terms of this Agreement only with respect to such Open Source Software, and not to the entire Product, including without limitation, any provisions governing attribution, access to source code, modification and reverse-engineering.

2.5 No Additional Terms. No shrink-wrap, click-acceptance or other terms and conditions outside this Agreement provided with any Licensed Materials or any part thereof ("**Additional Terms**") will be binding on Buyer or its Users, even if use of the Licensed Materials, or any part thereof, requires an affirmative "acceptance" of such Additional Terms before access to or use of the Licensed Materials, or any part thereof, is permitted. All such Additional Terms will be of no force or effect and will be deemed rejected by Buyer in their entirety. For clarity, the Product Listing and or Documentation are not Additional Terms subject to this Section.

2.6 High-Risk Activities. The Product is not designed or developed for use in highrisk, hazardous environments requiring fail-safe performance, including without limitation in the operation of nuclear facilities, aircraft navigation or control systems, air traffic control, or weapons systems, or any other application in which the failure of the Product could lead to severe physical or environmental damages ("**High Risk Activities**"). Buyer will not use the Product for any High Risk Activities.

3. Services.

3.1 SaaS Service. If Buyer is purchasing a SaaS Service Subscription, Licensor will provide the Product to Buyer as a SaaS Service in accordance with the Product Listing promptly following purchase of the Subscription and continuing until termination of the Subscription. Licensor will provide Buyer all license keys, access credentials and passwords necessary for access and use of the Product via the SaaS Service ("**Keys**") as set forth in the Product Listing.

3.2 Support Services. Licensor will make available to Buyer Documentation concerning the use and operation of the Product, and Licensor will provide Support Services to Buyer as described, incorporated or referenced in the Product Listing.

4. Proprietary Rights.

4.1 Licensed Materials. Subject to the licenses granted herein, Licensor will retain all right, title and interest it may have in and to the Licensed Materials, including all Proprietary Rights therein. Nothing in this Agreement will be construed or interpreted as granting to Buyer any rights of ownership or any other proprietary rights in or to the Licensed Materials or any Proprietary Rights therein.

4.2 Feedback. Buyer may, at its option, provide suggestions, ideas, enhancement requests, recommendations or feedback regarding the Licensed Materials or Support Services ("**Feedback**"), provided however, that Feedback does not include any Proprietary Rights of Buyer or Buyer's Affiliates or any Buyer Data or Buyer Materials. Licensor may use and incorporate Feedback in Licensor's products and services without compensation or accounting to Buyer, provided that neither Licensor nor its use of the Feedback identifies Buyer as the source of such Feedback. Feedback is not confidential to Buyer. Buyer will have no obligation to provide Feedback, and all Feedback is provided by Buyer "as is" and without warranty of any kind.

5. Warranties.

5.1 Licensed Materials. Licensor represents and warrants to Buyer that: (a) for Subscriptions with Entitlement Pricing, in the case of Product, or a component of a Product, deployed in the Buyer's Computing Environment, the Product or component will conform, in all material respects, to the Documentation, for 30 days after Buyer's purchase of the Subscription or the term of the Subscription, whichever is shorter, and, in the case of Product, or a component of a Product, deployed as a SaaS Service, the Product will conform, in all material respects, to the Documentation during the term of the Subscription; (b) a Product, or a component of a Product, provisioned for deployment in the Buyer's Computing Environment will not contain any automatic shut-down, lockout, "time bomb" or similar mechanisms that could interfere with Buyer's exercise of its rights under this Agreement (for clarity, the foregoing does not prohibit Keys that expire at the end of the Subscription); (c) Licensor will use industry standard practices designed to detect and protect the Product against any viruses, "Trojan horses", "worms", spyware, adware or other harmful code designed or used for unauthorized access to or use, disclosure, modification or destruction of information within the Product or interference with or harm to the operation of the Product or any systems, networks or data, including as applicable scanning the Product for malware and other security vulnerabilities and with up to date scanning software or service prior to making the Product (including any Product provided through Support Services) available to Buyer, and for Product or a component of a Product deployed via SaaS Service, scanning the Product or component on a regular basis; and (d) the Product, and Buyer's use thereof as permitted under this Agreement, will not be subject to any license or other terms that require that any Buyer Data, Buyer Materials or any software, documentation, information or other materials integrated, networked or used by Buyer with the Product, in whole or in part, be disclosed or distributed in source code form, be licensed for the purpose of making derivative works, or be redistributable at no charge.

5.2 **Services**. Licensor represents and warrants that any Support Services will be performed in a professional manner with a level of care, skill and diligence performed by experienced and knowledgeable professionals in the performance of similar services and in accordance with the Product Listing and Documentation.

5.3 **Remedies**. If any Product or Service fails to conform to the foregoing warranties, Licensor promptly will, at its option and expense, correct the Product and re-perform the Services as necessary to conform to the warranties. If Licensor does not correct the Product or re-perform the Services to conform to the warranties within a reasonable time, not to exceed 30 days (or such other period as may be agreed upon by the Parties) (the "**Cure Period**"), as Buyer's sole remedy and Licensor's exclusive liability (except as provided in Section 9), Buyer may for a period of 30 days following the conclusion of the Cure Period (or such other period as may be agreed upon by the Parties), elect to terminate the Subscription and this Agreement without further liability and Licensor will provide Buyer with a refund of any fees prepaid to Licensor by Buyer, prorated for the portion of the Subscription unused at the time Buyer reported the breach of warranty to Licensor, as well as, if applicable, any service credits available under Licensor's Support Services or other policies.

5.4 **Warranty Exclusions**. Licensor will have no liability or obligation with respect to any warranty to the extent attributable to any: (a) use of the Product by Buyer in violation of this Agreement or applicable Law; (b) modifications to the Licensed Materials not provided by Licensor or its Personnel; (c) use of the Product in combination with third-party equipment or software not provided or made accessible by Licensor or contemplated by the Product Listing or Documentation; or (d) use by Buyer of Product in conflict with the Documentation, to the extent that such nonconformity would not have occurred absent such use or modification by Buyer.

5.5 **Compliance with Laws**. Each Party represents and warrants to the other Party that it will comply with all applicable international, national, state and local laws, ordinances, rules, regulations and orders, as amended from time to time ("**Laws**") applicable to such Party in its performance under this Agreement.

5.6 **Power and Authority**. Each Party represents and warrants to the other Party that: (a) it has full power and authority to enter in and perform this Agreement and that the execution and delivery of this Agreement has been duly authorized; and (b) this

Agreement and such Party's performance hereunder will not breach any other agreement to which the Party is a party or is bound or violate any obligation owed by such Party to any third party.

5.7 Disclaimer. EXCEPT FOR THE WARRANTIES SPECIFIED IN THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE LICENSED MATERIALS, SERVICES, BUYER MATERIALS AND BUYER DATA, AND EACH PARTY HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. LICENSOR DOES NOT WARRANT: (A) THAT THE LICENSED MATERIALS WILL MEET BUYER'S REQUIREMENTS; OR (B) THAT THE OPERATION OF THE PRODUCT WILL BE UNINTERRUPTED OR ERROR FREE.

6. Confidentiality.

6.1 Confidential Information. "**Confidential Information**" means any nonpublic information directly or indirectly disclosed by either Party (the "**Disclosing Party**") to the other Party (the "**Receiving Party**") or accessible to the Receiving Party pursuant to this Agreement that is designated as confidential or that, given the nature of the information or the circumstances surrounding its disclosure, reasonably should be considered as confidential, including without limitation technical data, trade secrets, know-how, research, inventions, processes, designs, drawings, strategic roadmaps, product plans, product designs and architecture, security information, marketing plans, pricing and cost information, marketing and promotional activities, business plans, customer and supplier information, employee and User information, business and marketing plans, and business processes, and other technical, financial or business information, and any third party information that the Disclosing Party is required to maintain as confidential. Confidential Information will not, however, include any information which: (a) was publicly known or made generally available to the public prior to the time of disclosure; (b) becomes publicly known or made generally available after disclosure through no fault of the Receiving Party; (c) is in the possession of the Receiving Party, without restriction as to use or disclosure, at the time of disclosure by the Disclosing Party; (d) was lawfully received, without restriction as to use or disclosure, from a third party (who does not have an obligation of confidentiality or restriction on use itself); or (e) is developed by the Receiving Party independently from this Agreement and without use of or reference to the Disclosing Party's Confidential Information or Proprietary Rights. Except for rights expressly granted in this Agreement, each Party reserves all rights in and to its Confidential Information. The Parties agree that the Licensed Materials are Confidential Information of Licensor.

6.2 Obligations. The Parties will maintain as confidential and will avoid disclosure and unauthorized use of Confidential Information of the other Party using reasonable precautions. Each Party will protect such Confidential Information with the same degree of care that a prudent person would exercise to protect its own confidential information of a like nature, and to prevent the unauthorized, negligent, or inadvertent use, disclosure, or publication thereof or access thereto. Each Party will restrict Confidential Information to individuals who need to know such Confidential Information and who are bound to confidentiality obligations at least as protective as the restrictions described in this Section 6. Except as otherwise permitted under this Agreement, neither Party will use Confidential Information of the other Party for any purpose except in fulfilling its obligations or exercising its rights under this Agreement or as necessary for proper use of the Product. Each Party will promptly notify the other Party if it becomes aware of any unauthorized use or disclosure of the other Party's Confidential Information, and reasonably cooperate with the other Party in attempts to limit disclosure.

6.3 Compelled Disclosure. If and to the extent required by applicable Law, including regulatory requirements, discovery request, subpoena, court order or governmental action, the Receiving Party may disclose or produce Confidential Information but will give reasonable prior notice (and where prior notice is not permitted by applicable Law, notice will be given as soon as the Receiving Party is legally permitted) to the Disclosing Party to permit the Disclosing Party to intervene and to request protective orders or confidential treatment therefor or other appropriate remedy regarding such disclosure. Disclosure of any Confidential Information pursuant to any legal requirement will not be deemed to render it non-confidential, and the Receiving Party's obligations with respect to Confidential Information of the Disclosing Party will not be changed or lessened by virtue of any such disclosure. Notwithstanding any provisions herein, if Buyer is a Government Entity, Buyer will comply with all Laws applicable to it with respect to disclosure of public information.

6.4 NDA. Buyer and Licensor may agree to a separate nondisclosure agreement between Buyer and Licensor (or the respective Affiliates of Buyer and Licensor) ("**NDA**") that applies to disclosures occurring during the term of the Subscription, in which case the terms and conditions thereof are incorporated herein by reference and will apply instead of subsections 6.1 through 6.3 of this Section 6.

7. Additional SaaS Service Obligations and Responsibilities. This Section 7 applies to Subscriptions for Product, or a component of a Product, deployed via SaaS Service only.

7.1 Acceptable Use; Restrictions on Sensitive Information.

7.1.1 Buyer will not intentionally use the Product, component or SaaS Service

to: (a) store, download or transmit infringing or illegal content, or any viruses, "Trojan horses" or other harmful code; (b) engage in phishing, spamming, denial-of-service attacks or fraudulent or illegal activity; (c) interfere with or disrupt the integrity or performance of the Product, component or data contained therein or on Licensor's system or network or circumvent the security features of the Product; or (d) perform penetration testing, vulnerability testing or other security testing on the Product, component or Licensor's systems or networks or otherwise attempt to gain unauthorized access to the Product or Licensor's systems or networks.

7.1.2 Buyer will not use the SaaS Services to store or process Highly Sensitive Information unless Licensor specifically purchases a SaaS Service Subscription designed to be used with Highly Sensitive Information. "**Highly Sensitive Information**" means, for purposes of this Agreement: (1) "special categories of personal data," "sensitive personal information," or "Sensitive Personal Data," as defined under applicable Data Protection Law, including European Union Regulation 2016/679, Article 9(1) or any successor legislation; (2) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act (as amended and supplemented) ("**HIPAA**"); or (3) other information subject to additional protections or regulation under specific laws such as the Children's Online Privacy Protection Act or Gramm-Leach-Bliley Act (or related rules or regulations). Supplier shall have no responsibility for Highly Sensitive Information where the SaaS Service is not approved by Licensor to be used with Highly Sensitive Information.

7.1.3 Licensor may suspend Buyer's or a User's right to access or use any portion or all of the SaaS Service immediately upon notice to Buyer (a) if Licensor, after reasonable due diligence given the nature and severity of the issue, reasonably determines that: (i) Buyer or a User's use of the SaaS Service poses a material risk to the security or operation of Licensor's systems, the SaaS Service or the systems or data of any other customer, or (ii) Buyer or a User's use of the SaaS Service violates this Section 7.1 or is illegal or fraudulent; (b) if Buyer fails to pay any undisputed amounts within 30 days after notice of past due amounts; or (c) if Buyer uses a SaaS Service Subscription to store or process Highly Sensitive Information if such SaaS Service is not approved by Licensor to be used with Highly Sensitive Information. To the extent reasonably practicable, Licensor will limit the suspension of the SaaS Service pursuant to subsection (a) as needed to mitigate the applicable risk. Licensor will promptly restore the SaaS Service to Buyer upon resolution of the issue and/or payment of the outstanding amounts (as applicable).

7.2 Buyer Data and Buyer Materials.

7.2.1 Buyer is and will continue to be the sole and exclusive owner of all Buyer Materials, Buyer Data and other Confidential Information of Buyer, including all Proprietary Rights therein. Nothing in this Agreement will be construed or interpreted as granting to Licensor any rights of ownership or any other proprietary rights in or to the Buyer Data and Buyer Materials.

7.2.2 Buyer represents and warrants to Licensor that it has or will obtain all necessary consents, authorizations and rights and provide all necessary notices and disclosures in order to provide Buyer Data to Licensor and for Licensor to use Buyer Data in the performance of its obligations in accordance with the terms and condition of this Agreement, including any access or transmission to third parties with whom Buyer shares or permits access to Buyer Data.

7.2.3 The Parties agree that Buyer Data and Buyer Materials are Confidential Information of Buyer. Buyer hereby grants to Licensor a nonexclusive, nontransferable (except in connection with an assignment permitted under Section 12.2), revocable license, under all Proprietary Rights, to reproduce and use Buyer Materials and Buyer Data solely for the purpose of, and to the extent necessary for, performing Licensor's obligations under this Agreement. In no event will Licensor access, use or disclose to any third party any Buyer Data or any Buyer Materials for any purpose whatsoever other than as necessary for the purpose of providing the Product and Services to Buyer and performing its obligations under this Agreement. Licensor will not aggregate, anonymize or create any data derivatives of Buyer Data other than as necessary to provide the Product or Services and to perform its obligations in accordance with the terms and conditions of this Agreement.

7.2.4 Buyer will have full access to, and has the right to review and retain, the

entirety of Buyer Data contained in the Product. At no time will any computer or electronic records containing Buyer Data be stored or held in a form or manner not readily accessible to Buyer through the ordinary operation of the Product, except for backups of Buyer Data stored and/or maintained at Buyer's direction or in accordance with the Documentation and Privacy and Security Terms. Licensor will provide to Buyer all passwords, codes, comments, Keys and other documentation necessary for such access and use of the Product, and Buyer will be entitled to delete, or have Licensor delete, Buyer Data as expressly specified by Buyer.

7.3 **System Data**. To the extent that System Data identifies or permits, alone or in conjunction with other data, identification, association, or correlation of or with Buyer, its Affiliates, Users, customers, suppliers or other persons interacting with any of the foregoing, or any Confidential Information of Buyer or any device as originating through or interacting with Buyer or its Affiliates ("**Identifiable System Data**"), Licensor may only collect and use Identifiable System Data internally to administer, provide and improve the Product and Services as a generally available service offering, to identify opportunities for Buyer to optimize its use of the Product, including the provision of additional training, and to identify to Buyer complementary uses of Licensor's other products and services. Licensor will not target any data analysis at, or otherwise use any Identifiable System Data to derive or attempt to derive information regarding, Buyer and its Affiliates, their businesses, operations, finances, users, customers, prospective customers, suppliers or other persons interacting with Buyer and its Affiliates. Licensor will not target any development efforts arising from its use of Identifiable System Data at any person on the basis of the intended recipient's relationship with Buyer or any of its Affiliates or the intended recipient being in same industry or market as Buyer or any of its Affiliates. Licensor will not use or disclose any Identifiable System Data for any purpose other than as permitted in this Section unless otherwise agreed in writing by the Parties, and will, except for the use permitted in this Section, maintain the confidentiality and security of Identifiable System Data as Confidential Information.

7.4 Use of Other Data. Notwithstanding the foregoing, nothing in this Agreement will restrict: (a) Licensor's use of System Data or data derived from System Data that does not identify or permit, alone or in conjunction with other data, identification, association, or correlation of or with (i) Buyer, its Affiliates, Users, customers, suppliers or other persons interacting with Buyer and its Affiliates or any Confidential Information of Buyer, or (ii) any device (e.g. computer, mobile telephone, or browser) used to access or use the Product as originating through Buyer or its Affiliates or interacting with Buyer or its Affiliates; or (b) either Party's use of any data, records, files, content or other information related to any third party that is collected, received, stored or maintained by a Party independently from this Agreement.

7.5 Security; Breach Notification. Licensor will comply with the security practices (if any) incorporated or referenced in the Product Listing and Documentation for the Product, provided however that at all times Licensor will, consistent with industry standard practices, implement and maintain physical, administrative and technical safeguards and other security measures: (a) to maintain the security and confidentiality of Buyer Data; and (b) to maintain the availability and integrity of Buyer Data and to protect Buyer Data from known or reasonably anticipated threats or hazards to its security, including accidental loss, unauthorized use, access, alteration or disclosure. Licensor will inform Buyer promptly upon discovery of any material unauthorized access to, any unauthorized loss, use or disclosure of any Buyer Data (a "**Security Incident**"), provided that such notification is not prohibited by Law. Licensor will investigate the cause of the Security Incident and take reasonable steps to prevent further unauthorized access, loss, use or disclosure of Buyer Data. At Buyer's request and cost, Licensor will reasonably cooperate with Buyer in complying with its obligations under applicable law pertaining to responding to a Security Incident. Licensor's obligation to report or respond to a Security Incident under this Section is not an acknowledgement by Licensor of any fault or liability with respect to the Security Incident.

7.6 Data Protection Legislation.

7.6.1 Each Party will comply with all Data Protection Laws, and any implementations of such Laws, applicable to its performance under this Agreement. The Parties acknowledge and agree that they will consider in good faith implementing any codes of practice and best practice guidance issued by relevant authorities as they apply to applicable country specific Data Protection Laws or their implementations.

7.6.2 Without limiting the generality of the foregoing, if Licensor is collecting or furnishing Personal Data to Buyer or if Licensor is Processing Personal Data on behalf of Buyer, then Licensor and Buyer and/or their Affiliate(s), as applicable, will agree to supplemental privacy and security terms consistent with applicable Data Protection Law. Unless Licensor and Buyer expressly agree to be bound by other terms and conditions that reflect their respective legal obligations with respect to Personal Data, Licensor and Buyer agree to the terms and conditions of the attached Data Processing Addendum. For the avoidance of doubt, no

Personal Data should be processed or transferred under this Agreement without Privacy and Security Terms necessary for compliance with applicable Data Protection Law.

7.7 Remedies. Each Party agrees that in the event of a breach or threatened breach of this Section 7, the non-breaching Party will be entitled to injunctive relief against the breaching Party in addition to any other remedies to which the non-breaching Party may be entitled.

8. Limitations of Liability.

8.1 Disclaimer; General Cap. SUBJECT TO SECTIONS 8.2, 8.3 AND 8.4, IN NO

EVENT WILL (a) EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, WHETHER SUCH DAMAGES ARE BASED IN CONTRACT, TORT OR OTHER LEGAL THEORY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND (b) EITHER PARTY'S AGGREGATE LIABILITY UNDER THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES FROM CLAIMS BASED IN CONTRACT, TORT OR OTHER LEGAL THEORY, EXCEED THE FEES AND OTHER AMOUNTS PAID AND REQUIRED TO BE PAID UNDER THIS AGREEMENT IN THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO THE LIABILITY.

8.2 Exception for Gross Negligence, Willful Misconduct or Fraud. THE EXCLUSIONS OF AND LIMITATIONS ON LIABILITY SET FORTH IN SECTION 8.1(a) AND (b) WILL NOT APPLY TO A PARTY'S GROSS NEGLIGENCE, WILLFUL MISCONDUCT, OR FRAUD.

8.3 Exception for Certain Indemnification Obligations. THE EXCLUSIONS OF

AND LIMITATIONS ON LIABILITY SET FORTH IN SECTIONS 8.1(a) AND (b) WILL NOT APPLY TO ANY COSTS OF DEFENSE AND ANY AMOUNTS AWARDED AGAINST THE INDEMNIFIED PARTY BY A COURT OF COMPETENT JURISDICTION OR AGREED UPON PURSUANT TO SETTLEMENT AGREEMENT THAT ARE SUBJECT TO SUCH PARTY'S INDEMNIFICATION AND DEFENSE OBLIGATIONS UNDER THIS AGREEMENT.

8.4 Special Cap for Security Breach.

8.4.1 FOR SAAS SERVICE SUBSCRIPTIONS, THE EXCLUSIONS OF AND

LIMITATIONS ON LIABILITY SET FORTH IN SECTIONS 8.1(a) AND (b) WILL NOT APPLY TO, AND INSTEAD SECTION 8.4.2 WILL APPLY TO: (a) GOVERNMENT FINES AND PENALTIES INCURRED BY BUYER AND BUYER'S OUT-OF-POCKET, REASONABLE AND DOCUMENTED COSTS OF INVESTIGATION, NOTIFICATION, REMEDIATION AND MITIGATION SPECIFIED IN SECTION 9.5 RESULTING FROM ANY SECURITY INCIDENT RESULTING FROM BREACH OF LICENSOR'S

OBLIGATIONS UNDER THE PRIVACY AND SECURITY TERMS OR ANY VIOLATION BY LICENSOR OF DATA PROTECTION LAWS, AND LICENSOR'S OBLIGATIONS WITH RESPECT THERETO PURSUANT TO SECTION 9.5; AND (b) ANY LIABILITIES ARISING FROM CLAIMS BROUGHT BY THIRD PARTIES AGAINST BUYER ARISING FROM ANY SECURITY INCIDENT RESULTING FROM BREACH OF LICENSOR'S OBLIGATIONS UNDER ANY PRIVACY AND SECURITY TERMS OR ANY VIOLATION BY LICENSOR OF DATA PROTECTION LAWS, INCLUDING OUT-OF-POCKET COSTS OF DEFENSE AND ANY AMOUNTS AWARDED AGAINST BUYER BY A COURT OF COMPETENT JURISDICTION OR AGREED UPON PURSUANT TO A SETTLEMENT AGREEMENT.

8.4.2 FOR SAAS SERVICE SUBSCRIPTIONS, LICENSOR'S AGGREGATE LIABILITY UNDER THIS AGREEMENT FOR ANY SECURITY INCIDENT RESULTING FROM BREACH OF LICENSOR'S OBLIGATIONS UNDER ANY PRIVACY AND SECURITY TERMS OR RESULTING FROM BREACH OF LICENSOR'S OBLIGATIONS UNDER THE PRIVACY AND SECURITY TERMS OR ANY VIOLATION BY LICENSOR OF DATA PROTECTION LAWS, INCLUDING GOVERNMENT FINES AND PENALTIES INCURRED BY BUYER AND BUYER'S OUT-OF-POCKET, REASONABLE AND DOCUMENTED COSTS SET FORTH IN SECTION 9.5 AND LICENSOR'S INDEMNIFICATION AND DEFENSE OBLIGATIONS PURSUANT TO SECTION 9.1(b) AND ITS OBLIGATIONS PURSUANT TO SECTION 9.5 AND LICENSOR'S OBLIGATIONS WITH RESPECT THERETO PURSUANT TO SECTION 9.5, WHETHER SUCH DAMAGES ARE BASED IN CONTRACT, TORT OR OTHER LEGAL THEORY, WILL NOT EXCEED (IN LIEU OF AND NOT IN ADDITION TO THE AMOUNT SET FORTH IN SECTION 8.1) THREE TIMES THE FEES AND OTHER AMOUNTS PAID AND REQUIRED TO BE PAID UNDER THIS AGREEMENT IN THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO THE DAMAGES.

9. Indemnification.

9.1 Licensor Indemnity. Licensor will, at its expense, defend Buyer and its Affiliates and their respective officers, directors, employees, agents and representatives (collectively "**Buyer Indemnified Parties**") from and against any and all claims, actions, proceedings and suits brought by a third party (including government investigations), ("**Claims**") to the extent arising out of or alleging of any of the following: (a) infringement, misappropriation or violation of any Proprietary Rights by the Licensed Materials or Buyer's use thereof as permitted under this Agreement; and (b) any unauthorized access, use or disclosure of Buyer Data resulting from breach of Licensor's obligations under the Privacy and Security Terms or any violation by Licensor of Data Protection Laws. Licensor will pay all costs, damages and amounts finally awarded by a court or agreed upon in settlement (as set forth in Section 9.3 below) and any government fines and penalties assessed against or incurred by Buyer in any such Claims.

9.2 Buyer Indemnity. Buyer will, at its expense, defend Licensor and its Affiliates and their respective officers, directors, employees, agents and representatives (collectively "**Licensor Indemnified Parties**") from and against any and all Claims to the extent arising out of or alleging of any of the following: (a) infringement, misappropriation or violation of any Proprietary Rights by the Buyer Materials or Buyer Data or Licensor's use thereof as permitted under this Agreement; and (b) any unauthorized or unlawful Processing of Buyer Data by Licensor in the performance of its obligations as permitted under this Agreement resulting from any inaccuracy or breach of Buyer's representations, warranties, and/or obligations under Section 7.2.2. Buyer will pay all costs, damages and amounts finally awarded by a court or agreed upon in settlement (as set forth in Section 9.3 below) and any government fines and penalties assessed against or incurred by Licensor in any such Claims. Notwithstanding any provisions herein to the contrary, if Buyer is a Government Entity, this Section 9.2 will not apply except as permitted by applicable Law.

9.3 Process. The party(ies) seeking indemnification pursuant to this Section 9 (each, an "**Indemnified Party**" and collectively, the "**Indemnified Parties**") will give the other Party (the "**Indemnifying Party**") prompt notice of each Claim for which it seeks indemnification, provided that failure or delay in providing such notice will not release the Indemnifying Party from any obligations hereunder except to the extent that the Indemnifying Party is prejudiced by such failure. The Indemnified Parties will give the Indemnifying Party their reasonable cooperation in the defense of each Claim for which indemnity is sought, at the Indemnifying Party's expense. The Indemnifying Party will keep the Indemnified Parties informed of the status of each Claim. An Indemnified Party may participate in the defense at its own expense. The Indemnifying Party will control the defense or settlement of the Claim, provided that the Indemnifying Party, without the Indemnified Parties' prior written consent: (a) will not enter into any settlement that; (i) includes any admission of guilt or wrongdoing by any Indemnified Party; (ii) imposes any financial obligations on any Indemnified Party that Indemnified Party is not obligated to pay under this Section 9; (iii) imposes any non-monetary obligations on any Indemnified Party; and (iv) does not include a full and unconditional release of any Indemnified Parties; and (b) will not consent to the entry of judgment, except for a dismissal with prejudice of any Claim settled as described in (a). The Indemnifying Party will ensure that any settlement into which it enters for any Claim is made confidential, except where not permitted by applicable Law.

9.4 Infringement Remedy. In addition to Licensor's obligations under Section 9.1, if the Product or other Licensed Materials is held, or in Licensor's opinion is likely to be held, to infringe, misappropriate or violate any Proprietary Rights, or, if based on any claimed infringement, misappropriation or violation of Proprietary Rights, an injunction is obtained, or in Licensor's opinion an injunction is likely to be obtained, that would prohibit or interfere with Buyer's use of the Licensed Materials under this Agreement, then Licensor will at its option and expense either: (a) procure for Buyer the right to continue using the affected Licensed Materials in accordance with the license granted under this Agreement; or (b) modify or replace the affected Licensed Materials so that the modified or replacement Licensed Materials are reasonably comparable in functionality, interoperability with other software and systems, and levels of security and performance and do not infringe, misappropriate or violate any third-party Proprietary Rights. If, in such circumstances, Licensor cannot not successfully accomplish any of the foregoing actions on a commercially reasonable basis, Licensor will notify Buyer and either Party may terminate the Subscription and this Agreement, in which case Licensor will refund to Buyer any fees prepaid to Licensor by Buyer prorated for the unused portion of the Subscription. For clarity, Licensor's indemnification and defense obligations under this Section include infringement Claims based on use of the Licensed Materials by Buyer Indemnified Parties following an initial infringement Claim except that, if Licensor responds to an infringement Claim by accomplishing the solution in (b), Licensor will have no obligation to defend and indemnify Buyer for infringement Claims arising from Buyer's use after the accomplishment of (b) of the infringing Licensed Materials for which Licensor provided modified or replacement Licensed Materials and a reasonable time to implement the modified or replacement Licensed Materials.

9.5 Security Breach Remedy. In the case of a SaaS Service Subscription, in addition to Licensor's obligations under Section 9.1, in the event of any Security Incident resulting from breach of Licensor's obligations under any Privacy and Security Terms or any violation by Licensor of Data Protection Laws, Licensor will pay the government fines and penalties and other out-of-pocket costs incurred by Buyer, to the extent reasonable and documented, for (a) investigating and responding to the Security Incident; (b) legal advice regarding the Security Incident; (c) providing notification to affected individuals, applicable government and relevant industry self-regulatory agencies and the media; (d) providing credit monitoring and/or identity theft services to affected individuals; (e) operating a call center to respond to questions from affected individuals; and (f) any other investigation, mitigation, remediation, or notification required by law or regulators to be undertaken by Buyer in response to such Security Incident.

9.6 Limitations.

9.6.1 Licensor will have no liability or obligation under this Section 9 with

respect to any infringement Claim to the extent attributable to any: (a) modifications to the Licensed Materials not provided by Licensor or its Personnel; (b) use of the Product in combination with third-party equipment or software not provided or made accessible by Licensor or not specifically referenced for use with the Licensed Materials by the Product Listing or Documentation; or (c) use of the Licensed Materials by Buyer in breach of this Agreement. Licensor's liability under this Section 9 with respect to any infringement Claim that is attributable to use of the Product in combination with third-party equipment or software provided or made accessible by Licensor or specifically referenced by the Product Listing or Documentation is limited to Licensor's proportional share of defense costs and indemnity liability based on the lesser of: (i) the value of the contribution of the Licensed Materials to the total value of the actual or allegedly infringing combination; or (ii) the relative contribution of the Licensed Materials to the actual or allegedly infringed claims (e.g., the Licensed Materials are alleged to satisfy one limitation of a claim with four separate limitations and Licensor would be responsible for a 25% share of the defense and indemnity obligations).

9.6.2 Buyer will have no liability or obligation under this Section 9 with respect to any infringement Claim to the extent attributable to any: (a) modifications to the Buyer Materials or Buyer Data not provided by Buyer or its Personnel; or (b) use of the Buyer Materials or Buyer Data by Licensor in breach of this Agreement.

9.6.3 This Section 9 states the entire liability of Licensor with respect to
infringement, misappropriation or violation of Proprietary Rights of third parties by any Licensed Materials or any part thereof or by any use thereof by Buyer, and this Section 9 states the entire liability of Buyer with respect to infringement, misappropriation or violation of Proprietary Rights of third parties by any Buyer Materials, Buyer Data or any part thereof or by any Processing thereof by Licensor.

9.7 Not Limiting. The foregoing indemnities will not be limited in any manner whatsoever by any required or other insurance coverage maintained by a Party.

10. Term and Termination.

10.1 Term. This Agreement will continue in full force and effect until conclusion of the Subscription, unless terminated earlier by either Party as provided by this Agreement.

10.2 Termination. Either Party may terminate the Subscription or this Agreement if the other Party materially breaches this Agreement and does not cure the breach within 30 days following its receipt of written notice of the breach from the non-breaching Party. In the case of a
SaaS Service Subscription, termination by Licensor pursuant to this Section does not prejudice Buyer’s right, and Licensor’s obligation, to extract or assist with the retrieval or deletion of Buyer Data as set forth in Section 10.3.2 following such termination.

10.3 Effect of Termination.

10.3.1 Upon termination or expiration of the Subscription or this Agreement, Buyer’s right to use the Product licensed under such Subscription will terminate, and Buyer’s access to the Product and Service provided under such Subscription may be disabled and discontinued. Termination or expiration of any Subscription purchased by Buyer from Licensor will not terminate or modify any other Subscription purchased by Buyer from Licensor.

10.3.2 Within 45 days (or such other period as may be agreed upon by the Parties) following termination or expiration of any SaaS Service Subscription for any reason and on Buyer’s written request at any time before termination or expiration, Licensor will extract from the Product and/or Licensor’s Computing Environment (as applicable) and return to Buyer all Buyer Data, or if Buyer is able directly to retrieve or delete Buyer Data using the SaaS Service, then for a period of 45 days (or such other period as may be mutually agreed upon by the Parties in writing) following termination or expiration of this Agreement for any reason, Buyer may retrieve or delete Buyer Data itself with support from Licensor as reasonably requested by Buyer. If Buyer retrieves or deletes Buyer Data itself, Licensor will assist Buyer, as reasonably requested by Buyer, in validating whether the retrieval or deletion was successful. Buyer Data must be provided or extractable in a then-current, standard nonproprietary format. Notwithstanding anything herein to the contrary, Licensor's duty to return or enable Buyer's retrieval or deletion of the Buyer Data pursuant to this Section 10.3.2 may be delayed but will not be discharged due to the occurrence of any Force Majeure Event (defined below). Following delivery to Buyer of the Buyer Data and Buyer's confirmation thereof, or Buyer's retrieval or deletion of Buyer Data and Licensor's validation thereof or expiration of the applicable period, whichever is soonest, Licensor may, and within a reasonable time thereafter will, permanently delete and remove Buyer Data (if any) from its electronic and hard copy records and will, upon Buyer's request, certify to such deletion and removal to Buyer in writing. If Licensor is not able to delete any portion of the Buyer Data or Buyer Confidential Information, it will remain subject to the confidentiality, privacy and data security terms of this Agreement.

10.3.3 Sections 4 (Proprietary Rights), 6 (Confidentiality), 7.2.1 (Buyer Data and Buyer Materials), 8 (Limitations of Liability), 9 (Indemnification), 10.3 (Effect of Termination), 11 (Insurance), 12 (General), and 13 (Definitions) and any perpetual license granted under this Agreement, together with all other provisions of this Agreement that may reasonably be interpreted or construed as surviving expiration or termination, will survive the expiration or termination of this Agreement for any reason; but the nonuse and nondisclosure obligations of Section 6 will expire five years following the expiration or termination of this Agreement, except with respect to, and for as long as, any Confidential Information constitutes a trade secret.

11. Insurance.

11.1 Coverages. Each Party will obtain and maintain appropriate insurance necessary for implementing and performing under this Agreement in accordance with applicable Law and in accordance with the requirements of this Section 11. Subject to Licensor's right to self-insure as described below, Licensor will at its own cost and expense, acquire and continuously maintain the following insurance coverage during the term of this Agreement and for one year after:

11.1.1 Commercial General Liability insurance, including all major coverage categories, including premises-operations, property damage, products/completed operations, contractual liability, personal and advertising injury with limits of $1,000,000 per occurrence and $2,000,000 general aggregate, and $5,000,000 products/completed operations aggregate;

11.1.2 Professional Liability insurance, covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering Services in connection with this Agreement including acts, errors or omissions in rendering computer or information technology Services, proprietary rights infringement, data damage/destruction/corruption, failure to protect privacy, unauthorized access, unauthorized use, virus transmission and denial of service from network security failures with a minimum limit of $2,000,000 each claim and annual aggregate;

11.1.3 If a SaaS Service Subscription, Cyber Liability or Technology Errors and Omissions, with limits of $2,000,000 each claim and annual aggregate, providing for protection against liability for: (a) system attacks; (b) denial or loss of service attacks; (c) spread of malicious software code; (d) unauthorized access and use of computer systems; (e) liability arising from loss or disclosure of personal or corporate confidential data; (f) cyber extortion; (g) breach response and management coverage; (h) business interruption; and (i) invasion of privacy; and

11.1.4 If a SaaS Service Subscription, Computer Crime Insurance with limits of $1,000,000 and Employee Theft/Buyer Insurance Coverage with limits of $500,000.

11.2 Umbrella Insurance; Self-Insurance. The limits of insurance may be satisfied by any combination of primary and umbrella/excess insurance. In addition, either Party may satisfy its insurance obligations specified in this Agreement through a self-insured retention program. Upon request by Buyer, Licensor will provide evidence of Licensor's self-insurance program in a formal declaration (on Licensor's letterhead, if available) that declares Licensor is self-insured for the type and amount of coverage as described in Section 11.1. Licensor's declaration may be in the form of a corporate resolution or a certified statement from a corporate officer or an authorized principal of Licensor. The declaration also must identify which required coverages are self-insured and which are commercially insured.

11.3 Certificates and Other Requirements. Prior to execution of this Agreement and annually thereafter during the term, Buyer may request that Licensor furnish to Buyer a certificate of insurance evidencing the coverages set forth above. Licensor's Commercial General Liability and any umbrella insurance relied upon to meet the obligations in this Section will be primary and non-contributory coverage and the policies will not contain any intra-insured exclusions as between insured persons or organizations. Licensor's Commercial General Liability policy will provide a waiver of subrogation in favor of Buyer and its Affiliates. The stipulated limits of coverage above will not be construed as a limitation of any potential liability to Buyer, and failure to request evidence of this insurance will not be construed as a waiver of Licensor's obligation to provide the insurance coverage specified.

12. General.

12.1 Applicable Law. This Agreement will be governed and interpreted under the laws of the State of New York, excluding the principles of conflict of laws thereof and of any other jurisdiction. The Parties agree that any legal action or proceeding relating to this Agreement will be instituted solely in the state and federal courts located in New York City, New York. Each Party irrevocably submits to the jurisdiction of such courts, and each Party waives any objection that it may have to the laying of the venue of any such action or proceeding in the manner provided in this Section. The Parties agree that the United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement.

12.2 Assignment. Neither Party may assign or transfer this Agreement or any rights or delegate any duties herein without the prior written consent of the other Party, which will not be reasonably withheld, delayed or conditioned. Notwithstanding the foregoing, and without gaining the other Party's written consent, Licensor may assign this Agreement, in its entirety, and delegate its obligations to its Affiliates or to any entity acquiring all or substantially all of its assets, whether by sale of assets, sale of stock, merger or otherwise and Buyer may assign this Agreement, in its entirety, to any Affiliates or entity acquiring all or substantially all of its assets related to Buyer's account or the Buyer's entire business, whether by sale of assets, sale of stock, merger or otherwise. Any attempted assignment, transfer or delegation in contravention of this Section will be null and void. This Agreement will inure to the benefit of the Parties hereto and their permitted successors and assigns.

12.3 Entire Agreement. This Agreement constitutes the entire agreement between the Parties relating to the subject matter hereof, and there are no other representations, understandings or agreements between the Parties relating to the subject matter hereof This Agreement is solely between Buyer and Licensor. Neither Amazon Web Services, Inc. nor any of its Affiliates are a party to this Agreement and none of them will have any liability or obligations hereunder. The terms and conditions of this Agreement will not be changed, amended, modified or waived unless such change, amendment, modification or waiver is in writing and signed by authorized representatives of the Parties. NEITHER PARTY WILL BE BOUND BY, AND EACH SPECIFICALLY OBJECTS TO, ANY PROVISION THAT IS DIFFERENT FROM OR IN ADDITION TO THIS AGREEMENT (WHETHER PROFFERED ORALLY OR IN ANY QUOTATION, PURCHASE ORDER, INVOICE, SHIPPING DOCUMENT, ONLINE TERMS AND CONDITIONS, ACCEPTANCE, CONFIRMATION, CORRESPONDENCE, OR OTHERWISE), UNLESS SUCH PROVISION IS SPECIFICALLY AGREED TO IN A WRITING SIGNED BY BOTH PARTIES.

12.4 Export Laws. Each Party will comply with all applicable customs and export control laws and regulations of the United States and/or such other country, in the case of Buyer, where Buyer or its Users use the Product or Services, and in the case of Licensor, where Licensor provides the Product or Services. Each Party certifies that (i) it and its Personnel are not on any of the relevant U.S. Government Lists of prohibited persons, including but not limited to the Treasury Department's List of Specially Designated Nationals and the Commerce Department's list of Denied Persons and (ii) neither it nor its Personnel are the subject or target of any sanctions program, including but not limited to the sanctions programs of the U.S., the European Union, and UN Security Council. Neither Party will export, re-export, ship, or otherwise transfer the Licensed Materials, Services or Buyer Data to any country subject to an embargo or other sanction by the United States or other applicable jurisdiction.

12.5 Force Majeure. Neither Party will be liable hereunder for any failure or delay in the performance of its obligations in whole or in part, on account of riots, fire, flood, earthquake, explosion, epidemics, war, strike or labor disputes (not involving the Party claiming force majeure), embargo, civil or military authority, act of God, governmental action or other causes beyond its reasonable control and without the fault or negligence of such Party or its Personnel and such failure or delay could not have been prevented or circumvented by the non-performing Party through the use of alternate sourcing, workaround plans or other reasonable precautions (a "**Force Majeure Event**"). If a Force Majeure Event continues for more than 14 days for any Subscription with Entitlement Pricing, Buyer may cancel the unperformed portion of the Subscription and receive a pro rata refund of any fees prepaid by Buyer to Licensor for such unperformed portion.

12.6 Government Rights. As defined in FARS §2.101, the Product and Documentation are "commercial items" and according to DFARS §252.227 and 7014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation". Consistent with FARS §12.212 and DFARS §227.7202, any use, modification, reproduction, release, performance, display or discourse of such commercial software or commercial software documentation by the U.S. government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

12.7 Headings. The headings throughout this Agreement are for reference purposes only, and the words contained therein will in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

12.8 No Third-Party Beneficiaries. Except as specified in Section 9 with respect to Buyer Indemnified Parties and Licensor Indemnified Parties, nothing express or implied in this Agreement is intended to confer, nor will anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations or liabilities whatsoever.

12.9 Notices. To be effective, notice under this Agreement must be given in writing. Each Party consents to receiving electronic communications and notifications from the other Party in connection with this Agreement. Each Party agrees that it may receive notices from the other Party regarding this Agreement: (a) by email to the email address designated by such Party as a notice address for the Standard Contract; (b) by personal delivery; (c) by registered or certified mail, return receipt requested; or (d) by nationally recognized courier service. Notice will be deemed given upon written verification of receipt.

12.10 Nonwaiver. Any failure or delay by either Party to exercise or partially exercise any right, power or privilege under this Agreement will not be deemed a waiver of any such right, power or privilege under this Agreement. No waiver by either Party of a breach of any term, provision or condition of this Agreement by the other Party will constitute a waiver of any succeeding breach of the same or any other provision hereof No such waiver will be valid unless executed in writing by the Party making the waiver.

12.11 Publicity. Neither Party will issue any publicity materials or press releases that refer to the other Party or its Affiliates, or use any trade name, trademark, service mark or logo of the other Party or its Affiliates in any advertising, promotions or otherwise, without the other Party's prior written consent.

12.12 Relationship of Parties. The relationship of the Parties will be that of independent contractors, and nothing contained in this Agreement will create or imply an agency relationship between Buyer and Licensor, nor will this Agreement be deemed to constitute a joint venture or partnership or the relationship of employer and employee between Buyer and Licensor. Each Party assumes sole and full responsibility for its acts and the acts of its Personnel. Neither Party will have the authority to make commitments or enter into contracts on behalf of, bind, or otherwise oblige the other Party.

12.13 Severability. If any term or condition of this Agreement is to any extent held invalid or unenforceable by a court of competent jurisdiction, the remainder of this Agreement will not be affected thereby, and each term and condition will be valid and enforceable to the fullest extent permitted by law.

12.14 Subcontracting. Licensor may use Subcontractors in its performance under this Agreement, provided that: (a) Licensor remains responsible for all its duties and obligations hereunder and the use of any Subcontractor will not relieve or reduce any liability of Licensor or cause any loss of warranty under this Agreement; and (b) Licensor agrees to be directly liable for any act or omission by such Subcontractor to the same degree as if the act or omission were performed by Licensor such that a breach by a Subcontractor of the provisions of this Agreement will be deemed to be a breach by Licensor. The performance of any act or omission under this Agreement by a Subcontractor for, by or through Licensor will be deemed the act or omission of Licensor. Upon request, Licensor will identify to Buyer any Subcontractors performing under this Agreement, including any that have access to Buyer Data, and such other information reasonably requested by Buyer about such subcontracting.

13. Definitions.

13.1 "**Affiliate**" means, with respect to a Party, any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with such Party.

13.2 "**AWS Marketplace**" means the marketplace operated by Amazon Web Services, Inc., which is currently located at https://aws.amazon.com/marketplace/, as it may be updated or relocated from time to time.

13.3 "**Buyer Data**" means all data, Personal Data, records, files, information or content, including text, sound, video, images and software, that is (a) input or uploaded by Buyer or its Users to or collected, received, transmitted, processed, or stored by Buyer or its Users using the Product or SaaS Service in connection with this Agreement, or (b) derived from (a). Buyer Data is Confidential Information of Buyer.

13.4 "**Buyer Materials**" means any property, items or materials, including Buyer Data, furnished by Buyer to Licensor for Licensor's use in the performance of its obligations under this Agreement.

13.5 "**Buyer's Computing Environment**" means the Buyer computing environment in which Licensor authorizes use of the Subscription.

13.6 "**Contractor**" means any third party contractor of Buyer or other third party performing services for Buyer, including outsourcing suppliers.

13.7 "**Data Protection Law(s)**" means all data protection and privacy laws and regulations, now in effect or hereinafter enacted, in any jurisdiction of the world, and applicable to the Processing of Personal Data under the Agreement, including Regulation 2016/679 (General Data Protection Regulation) ("**GDPR**"), and Cal. Civ. Code 1798.100 et seq. (California Consumer Privacy Act) ("**CCPA**").

13.8 "**Documentation**" means the user guides, manuals, instructions, specifications, notes, documentation, printed updates, "read-me" files, release notes and other materials related to the Product (including all information included or incorporated by reference in the applicable Product Listing), its use, operation or maintenance, together with all enhancements, modifications, derivative works, and amendments to those documents, that Licensor publishes or provides under this Agreement.

13.9 "**Entitlement Pricing**" means any Subscription pricing model where Buyer purchases a quantity of usage upfront, including prepaid and installment payment pricing models.

13.10 "**Governmental Entity**" means the government of any nation or any political subdivision thereof, whether at the national, state, territorial, provincial, municipal, or any other level, including any agency, authority, regulatory body, court, central bank, or other governmental entity exercising executive, legislative, judicial, taxing, regulatory, or administrative powers or functions of government (including any supra-national bodies such as the European Union or the European Central Bank).

13.11 "**International Data Transfer Mechanism**" means the special protections that some jurisdictions require two or more parties that transfer information across international borders to adopt to make the transfer lawful, e.g., Standard Contractual Clauses, Binding Corporate Rules, or statutory obligations that require the parties to adopt certain technical, organizational, or contractual measures. "**Transfer**," in the context of an International Data Transfer Mechanism, means to disclose or move Personal Data from a storage location in one jurisdiction to another, or to permit a party in one jurisdiction to access Personal Data that the other party stores in another jurisdiction that requires an International Data Transfer Mechanism.

13.12 "**Licensed Materials**" means the Product, Documentation and any other items, materials or deliverables that Licensor provides, or is obligated to provide, as part of a Subscription.

13.13 "**Licensor's Computing Environment**" means the computing infrastructure and systems used by Licensor to provide the Product via SaaS Service.

13.14 "**Open Source Software**" means software distributed under a licensing or distribution model that is publicly available and makes the source code to such software available to licensees for use, modification and redistribution.

13.15 "**Personal Data**" means information the Buyer Data that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a natural person. "Personal Data" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Personal Information," as context requires, to the extent such information forms part of the Buyer Data.

13.16 "**Personnel**" means a Party or its Affiliate's directors, officers, employees, nonemployee workers, agents, auditors, consultants, contractors, subcontractors and any other person performing services on behalf of such Party (but excludes the other Party and any of the foregoing of the other Party).

13.17 "**Privacy and Security Terms**" means Section 7.5, the attached Data Protection Addendum (if applicable), and any other terms and conditions regarding the privacy and security of data agreed upon by the parties that are a part of this Agreement, whether in an addendum or amendment to this Standard Contract.

13.18 "**Process"** or **"Processing"** means any operation or set of operations that are performed on Personal Data, whether or not by automated means, including, but not limited to, accessing, collecting, recording, organizing, structuring, using, storing, transferring, retaining, disclosing, selling, sharing, deleting, and destroying Personal Data.

13.19 "**Product Listing**" means the description of Product and other product information listed on the AWS Marketplace and offered by Licensor or its authorized reseller, including Support Services and Licensor's policies and procedures incorporated or referenced in the product information. The Product Listing may also describe, incorporate or reference Licensor's security practices or disclosures concerning Open Source Software.

13.20 "**Product**" means the computer software and any associated data, content and/or services identified in the applicable Product Listing that Licensor provides or is obligated to provide as part of a Subscription, including any patches, bug fixes, corrections, remediation of security vulnerabilities, updates, upgrades, modifications, enhancements, derivative works, new releases and new versions of the foregoing that Licensor provides, or is obligated to provide, as part of the Subscription.

13.21 "**Proprietary Rights**" means all intellectual property and proprietary rights throughout the world, whether now known or hereinafter discovered or invented, including, without limitation, all: (a) patents and patent applications; (b) copyrights and mask work rights; (c) trade secrets; (d) trademarks; (e) rights in data and databases; and (f) analogous rights throughout the world.

13.22 "**SaaS Service**" means access and use of the Product, or a component of a Product, as deployed and hosted by Licensor in the Licensor's Computing Environment, and any software and other technology provided or made accessible by Licensor in connection therewith (and not as a separate product or service) that Buyer is required or has the option to use in order to access and use the Product.

13.23 "**Services**" means all services and tasks that Licensor provides or is obligated to provide under this Agreement, including without limitation Support Services.

13.24 "**Subcontractor**" means any third party subcontractor or other third party to whom Licensor delegates any of its duties and obligations under this Agreement.

13.25 "**Subscription**" means a Product subscription for a specific use capacity purchased by Buyer and fulfilled by Licensor for the licensing and provision of Product, whether deployed in Buyer's Computing Environment and/or provided as a SaaS Service through Licensor's Computing Environment.

13.26 "**Support Services**" means the support and maintenance services for the Product that Licensor provides, or is obligated to provide, as described in the Product Listing.

13.27 "**System Data**" means data and data elements (other than Buyer Data) collected by the Product, SaaS Service or Licensor's Computer Environment regarding configuration, environment, usage, performance, vulnerabilities and security of the Product or SaaS Service that may be used to generate logs, statistics and reports regarding performance, availability, integrity and security of the Product or SaaS Service.

13.28 "**User**" means Buyer, its Affiliates and any person or software program or computer systems authorized by Buyer or any of its Affiliates to access and use the Product as permitted under this Agreement, including Contractors of Buyer or its Affiliates.

Data Processing Addendum for
Standard Contract for AWS Marketplace

This Data Processing Addendum (this "**Addendum**") is part of the Standard Contract for AWS Marketplace (the "**Standard Contract**") between Licensor (who is the Processor) and Buyer (who is the Controller) and governs Licensor's Processing of Personal Data in its capacity as a

Processor in connection with Licensor's provision of the Services it provides pursuant to the Standard Contract. This Addendum shall only apply if Licensor and Buyer have not entered into a separate data processing agreement or similar contractual arrangement with respect to the Processing of Personal Data. All capitalized terms used but not defined in this Addendum have the meanings given to them in the Standard Contract.

Processing of Personal Data

I. DEFINITIONS

1. "**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Business" or "Third Party," as context requires.

2. "**Personal Data Breach**" means a confirmed Security Incident, such as a breach of security of the Services that caused an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, or an event that qualifies as a reportable data breach under applicable Data Protection Law.

3. "**Processor**" means an entity that processes personal data on behalf of another entity. "Processor" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Service Provider," as context requires.

4. "**Sensitive Personal Data**" means the following types and categories of Personal Data, as defined under applicable Data Protection Law, such as: (a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (b) genetic data; (c) biometric data; (d) data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; (e) data concerning a natural person's sex life or sexual orientation; (f) government identification numbers (e.g., SSNs, driver's license); (g) payment card information; (h) nonpublic personal information governed by the Gramm-Leach-Bliley Act; (i) an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and (j) precise geolocation. "Sensitive Personal Data" includes equivalent terms in other Data Protection Law, such as "special categories or personal data" or "sensitive personal information," as context requires.

II. INTERNATIONAL DATA TRANSFERS

1. **International Data Transfer**. Before Buyer transfers Personal Data to Licensor, or permits Licensor to access Personal Data located in a jurisdiction that requires an International Data Transfer Mechanism, Buyer will notify Licensor of the relevant requirement and the parties will work together in good faith to fulfill the requirements of that International Data Transfer Mechanism. The parties will institute and comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law.

III. DATA PROTECTION GENERALLY

1. Compliance. The parties will comply with their respective obligations under Data Protection Law and their respective privacy notices.

2. Confidentiality. Licensor will restrict access to Personal Data to those authorized persons who need such information to provide the Services. Such authorized persons are obligated to maintain the confidentiality of any Personal Data.

3. Security. Licensor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the Personal Data provided by Buyer and processed by Licensor. Such security measures will be at least as protective as the security requirements set forth in the Standard Contract. When choosing security controls, Licensor will consider the state of the art, the cost of implementation, the nature, scope, context, and purposes of Personal Data Processing, and the risk to data subjects of a Security Incident or Personal Data Breach affecting Personal Data.

4. Retention. Personal Data received from Buyer will be retained only for so long as may be reasonably required in connection with Licensor's performance of the Standard Contract or as otherwise required under Data Protection Law.

5. Cooperation. Licensor will cooperate to the extent reasonably necessary in connection with Buyer's requests related to data protection impact assessments and consultation with supervisory authorities and for the fulfillment of Buyer's obligation to respond to requests for exercising a data subject's rights under Data Protection Law. Licensor reserves the right to charge Buyer for its reasonable costs in collecting and preparing Personal Data for transfer and for any special arrangements for making the transfer.

6. Third Party Requests. If Licensor receives a request from a third party in connection with any government investigation or court proceeding that Licensor believes would require it to produce any Personal Data, Licensor will inform Buyer in writing of such request and cooperate with Buyer if Buyer wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable Law.

7. Instructions from the Buyer. Notwithstanding anything in the Standard Contract to the contrary, Licensor will only Process Personal Data in order to provide the Services to Buyer, in accordance with Buyer's written instructions, as permitted by the last sentence of Section III.8 below, or as required by applicable Law. Licensor will promptly inform Buyer if following Buyer instructions would result in a violation of Data Protection Law or where Licensor must disclose Personal Data in response to a legal obligation (unless the legal obligation prohibits Licensor from making such disclosure).

8. Scope of Processing. Licensor is prohibited from: (a) Selling (as such term is defined in the CCPA) Personal Data, (b) Processing the Personal Data for any purpose other than for the specific business purpose of performing Buyer's documented instructions for the business purposes defined in this Addendum, including retaining, using, or disclosing the Personal Data for a commercial purpose other than performing Buyer's instructions, or (c) Processing the Personal Data outside of the direct business relationship between the parties as defined in this Agreement. Licensor certifies that it understands these restrictions. Notwithstanding the foregoing, Licensor may Process Personal Data to retain or employ another person as a SubProcessor (as defined in Section III.10 below) in accordance with this Addendum, for internal use by the Licensor to improve the quality of its services (provided that Licensor does not use the Personal Data to perform services on behalf of another person), or to detect data Security Incidents or protect against malicious, deceptive, fraudulent or illegal activity.

9. Sensitive Information. Buyer will inform Licensor if Personal Data is Sensitive Personal Data.

10. Sub-processors. Buyer grants Licensor general authorization, as a Processor, to engage other processors ("**Sub-Processors**") to assist in providing the Services consistent with the Standard Contract. Licensor will make a list of such Sub-Processors accessible to Buyer prior to transferring any Personal Data to such Sub-Processors. Licensor will notify Buyer of any changes to the list of Sub-Processors by updating such list from time to time in order to give Buyer an opportunity to object to such changes.

11. Sub-processor Liability. Where Licensor engages a Sub-Processor for carrying out specific processing activities on behalf of Buyer, substantially similar data protection obligations as set out in this Addendum will be imposed on that Sub-Processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Law. Licensor will be liable for the acts or omissions of its Sub-Processors to the same extent as Licensor would be liable if performing the services of the Sub-Processor directly.

12. Recordkeeping. Upon a request issued by a supervisory authority for records regarding Personal Data, Licensor will cooperate to provide the supervisory authority with records related to processing activities performed on Buyer's behalf, including information on the categories of Personal Data Processed and the purposes of the Processing, the use of service providers with respect to such Processing, any data disclosures or transfers to third parties and a general description of technical and organizational measures to protect the security of such data.

13. Transfer of Personal Data; Appointment. Buyer authorizes Licensor to Process Personal Data in the United States or any other country in which Licensor or its Sub-Processors maintain facilities. Buyer appoints Licensor to perform any such transfer of Personal Data to any such country and to store and process Personal Data in order to provide the Services. Licensor will conduct all such activity in compliance with the Standard Contract, this Addendum, Data Protection Law, any applicable International Data Transfer Mechanism and Buyer instructions.

14. Deletion or Return. When instructed by Buyer, Licensor will delete any Personal Data or return it to Buyer in a secure manner and delete all remaining copies of Personal Data after such return except where otherwise required under applicable Law. Licensor will relay Buyer's instructions to all Sub-Processors.

15. Breach Notification. After becoming aware of a Personal Data Breach, Licensor will notify Buyer without undue delay of: (a) the nature of the Personal Data Breach; (b) the number and categories of data subjects and data records affected; and (c) the name and contact details for the relevant contact person at Licensor.

16. Audits. Upon request, Licensor will make available to Buyer all information necessary, and allow for and contribute to audits, including inspections, conducted by Buyer or another auditor mandated by Buyer, to demonstrate compliance with Data Protection Law. For clarity, such audits or inspections are limited to Licensor's Processing of Personal Data only, not any other aspect of Licensor's business or information systems. If Buyer requires Licensor to contribute to audits or inspections that are necessary to demonstrate compliance, Buyer will provide Licensor with written notice at least 60 days in advance of such audit or inspection. Such written notice will specify the things, people, places or documents to be made available. Such written notice, and anything produced in response to it (including any derivative work product such as notes of interviews), will be considered Confidential Information and, notwithstanding anything to the contrary in the Standard Contract, will remain Confidential Information in perpetuity or the longest time allowable by applicable Law after termination of the Standard Contract. Such materials and derivative work product produced in response to Buyer's request will not be disclosed to anyone without the prior written permission of Licensor unless such disclosure is required by applicable Law. If disclosure is required by applicable Law, Buyer will give Licensor prompt written notice of that requirement and an opportunity to obtain a protective order to prohibit or restrict such disclosure except to the extent such notice is prohibited by applicable Law or order of a court or governmental agency. Buyer will make every effort to cooperate with Licensor to schedule audits or inspections at times that are convenient to Licensor. If, after reviewing Licensor's response to Buyer's audit or inspection request, Buyer requires additional audits or inspections, Buyer acknowledges and agrees that it will be solely responsible for all costs incurred in relation to such additional audits or inspections.

AMENDMENT TO
STANDARD CONTRACT FOR AWS MARKETPLACE

This Amendment to the Standard Contract for AWS Marketplace (the **"Amendment"**) is part of the Standard Contract for AWS Marketplace (the "**Standard Contract**") between Buyer and Licensor. This Amendment amends and supplements the Standard Contract, the terms and conditions of which are incorporated herein by reference, as if expressly set forth herein.

Unless defined elsewhere in this Amendment, terms in initial capital letters have the meanings set forth in the Standard Contract.

1. **Product Subscription**. This Amendment applies to the following Subscription purchased by Buyer.

   [BC Mosaic SaaS]

2. **Amendment of Standard Contract.** The Parties agree that the Standard Contract is hereby amended as follows:

   a. **Amendment to Sections 2.1.1 and 2.1.2.** Sections 2.1.1 and 2.1.2 of the Standard Contract are hereby amended to strike the words "nonterminable" and instead define the license as revocable by Licensor pursuant to termination/revocation rights stated elsewhere in the Agreement.

   b. **Amendment to Section 2.1.3.** Section 2.1.3 of the Standard Contract is hereby amended as follows:

   2.1.3. Regardless of whether Buyer deploys the Product in Buyer's Computing Environment or accesses the Product via the SaaS Service, Buyer may use the Product only: (a) in support of the professional, authorized internal operations of Buyer's and its Affiliates' business(es) or organization(s) within the scope of the Subscription obtained; (b) in connection with Buyer's and its Affiliates' products and services (but, for clarity, not as a stand-alone product or service of Buyer or its Affiliates); (c) in connection with Buyer's and its Affiliate's interactions with Users; (d) after acceptance of the Agreement, as amended; and (e) provided that Buyer and any Users are authorized by their employer or organization to access the Licensed Materials. Buyer must, at all times, ensure compliance by itself, its Affiliate(s), and its User(s) with the following: (i) all access credentials must be kept strictly confidential; (ii) each User must log in using only their assigned, unique account and is responsible for all activities performed under their account; and (iii) notification to Licensor within no more than one (1) business day of any suspected or actual unauthorized access to the Product. Licensor may suspend or revoke access at its discretion for (i) security or compliance reasons, (ii) as a result of Buyer's (or their Affiliate(s) or User(s)) violation of the terms of the agreement, and/or (iii) in the event the relationship between Licensor and Buyer is terminated. In the event of such access revocation or termination, all buyer obligations related to confidentiality and data protection remain in full force and effect.

   c. **Amendment to Section 2.3.** Section 2.3 of the Standard Contract is hereby amended to include additional use restrictions, such that the revised clause will read, in its entirety, as follows:

   2.3. **Restrictions**. Except as specifically provided in this Agreement, Buyer and any other User of any Licensed Materials, in whole or in part, may not: (a) copy the Licensed Materials, in whole or in part; (b) distribute copies of Licensed Materials, in whole or in part, to any third party; (c) modify, adapt, translate, make alterations to or make derivative works based on Licensed Materials or any part thereof; (d) except as permitted by Law, decompile, reverse engineer, disassemble or otherwise attempt to derive source code, algorithms or the underlying structure of the Product; (e) use, rent, loan, sub-license, lease, distribute or attempt to grant other rights to any part of the Licensed Materials to third parties; (f) use the Licensed Materials to act as a consultant, service bureau or application service provider; (g) permit access of any kind to the Licensed Materials to any third party; (h) attempt to re-identify pseudonymised or anonymised data; (i) copy, download, export, or extract research data except as explicitly permitted; (j) circumvent security or access controls; (k) interfere with system functionality; (l) use the Licensed Materials for unlawful, unethical, or unauthorized purposes; or (m) upload harmful code or compromise system integrity.

d. Amendment to Section 2.5. Section 2.5 of the Standard Contract is hereby stricken in its entirety.

e. Amendment to Section 7.1.1. Section 7.1.1 of the Standard Contract is hereby amended to include additional access/use restrictions, such that the revised clause reads, in its entirety, as follows:

7.1.1. Buyer will not intentionally use the Product, component or SaaS Service to: (a) store, download or transmit infringing or illegal content, or any viruses, “Trojan horses” or other harmful code; (b) engage in phishing, spamming, denial-of-service attacks or fraudulent or illegal activity; (c) otherwise interfere with, compromise, or disrupt the integrity or performance of the Product, component or data contained therein or on Licensor’s system or network or circumvent the security features or access controls of the Product in any way; (d) perform penetration testing, vulnerability testing or other security testing on the Product, component or Licensor’s systems or networks or otherwise attempt to gain unauthorized access to the Product or Licensor’s systems or networks; (e) attempt to re-identify pseudonymised or anonymised data; (f) copy, download, export, or extract research data except as explicitly permitted; (g) interfere with system functionality; or (h) use the Licensed Materials for unlawful, unethical, or unauthorized purposes.

f. Amendment to Section 7.1.2. Section 7.1.2 of the Standard Contract is hereby amended to read as follows:

7.1.2. Buyer will not use the SaaS Services to store or process Highly Sensitive Information unless Buyer specifically purchases a SaaS Service Subscription designed to be used with Highly Sensitive Information. “**Highly Sensitive Information**” means, for purposes of this Agreement: (1) “special categories of personal data,” “sensitive personal information,” or “Sensitive Personal Data,” as defined under applicable Data Protection Law, including European Union Regulation 2016/679, Article 9(1) or any successor legislation; (2) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act (as amended and supplemented) (“**HIPAA**”); or (3) other information subject to additional protections or regulation under specific laws such as the Children’s Online Privacy Protection Act or Gramm-Leach-Bliley Act (or related rules or regulations). Supplier shall have no responsibility for Highly Sensitive Information where the SaaS Service is not approved by Licensor to be used with Highly Sensitive Information.

7.2. **Amendment to Section 8.** Section 8 of the Standard Contract is hereby amended to add a new section 8.5, which shall read, in its entirety, as follows:

> 8.5. **Exception for Breach of Confidentiality**. THE EXCLUSIONS OF AND LIMITATIONS ON LIABILITY SET FORTH IN SECTION 8.1(a) AND (b) WILL NOT APPLY TO ACTIONS BROUGHT AS A RESULT OF A PARTY'S BREACH OF CONFIDENTIALITY OBLIGATIONS SET FORTH IN SECTION 6 HERETO

7.3. **Amendment to Section 8.1.** Section 8.1 of the Standard Contract is hereby amended to add section 8.5 to the scope of sections noting exclusions.

7.4. **Amendment to Section 8.4.2.** Section 8.4.2 of the Standard Contract is hereby amended to limit the liability cap to two times (2X) the fees and other amounts paid and required to be paid under this Agreement in the 12 months preceding the event giving rise to the damages.

7.5. **Amendment to Section 9.2.** Section 9.2 of the Standard Contract is hereby amended to add the following item to the scope of Buyer Indemnity: and (c) any breach by Buyer of the use/access obligations contained in the agreement.

7.6. **Amendment to Section 10.2.** Section 10.2 of the Standard Contract is hereby amended to the following:

> **10.2 Termination**. In addition to the termination/revocation rights identified elsewhere in this Agreement, either Party may terminate the Subscription or this Agreement if the other Party materially breaches this Agreement and does not cure the breach within 30 days following its receipt of written notice of the breach from the non-breaching Party. In the case of a SaaS Service Subscription, termination by Licensor pursuant to this Section does not prejudice Buyer's right, and Licensor's obligation, to extract or assist with the retrieval or deletion of Buyer Data as set forth in Section 10.3.2 following such termination.

7.7. **Amendment to Section 11.1.1.** Section 11.1.1 of the Standard Contract is hereby amended to the following:

> **11.1.1.** Commercial General Liability insurance, including all major coverage categories, including premises-operations, property damage, products/completed operations, contractual liability, personal and advertising injury with limits of $1,000,000 per occurrence and $2,000,000 general aggregate, and $2,000,000 products/completed operations aggregate;

7.8. **Amendment to Section 11.1.3.** Section 11.1.3 of the Standard Contract is hereby amended to the following:

> **11.1.3.** If a SaaS Service Subscription, Cyber Liability or Technology Errors and Omissions, with an aggregate limit of $1,000,000, providing for protection against liability for: (a) system attacks; (b) denial or loss of service attacks; (c) spread of malicious software code; (d) unauthorized access and use of computer systems; (e) liability arising from loss or disclosure of personal or corporate confidential data; (f) cyber extortion; (g) breach response and management coverage; (h) business interruption; and (i) invasion of privacy

11.2. Amendment to Section 11.1.4. Section 11.1.4 of the Standard Contract is hereby stricken in its entirety.

11.3. Amendment to Section 12.1. Section 12.1 of the Standard Contract is hereby amended to specify that the applicable law and jurisdiction shall be Switzerland instead of the State of New York.

11.4. Amendment to Section 12.3. Section 12.3 of the Standard Contract is hereby amended to the following:

> **12.3 Entire Agreement**. This Agreement constitutes the entire agreement between the Parties relating to the subject matter hereof, and there are no other representations, understandings or agreements between the Parties relating to the subject matter hereof at the time of signing. Licensor may, however, periodically make updates to its terms and conditions. In such cases, Buyer will be notified of any material changes, and continued access/use of the Licensed Materials constitutes acceptance of such revised terms. This Agreement is solely between Buyer and Licensor. Neither Amazon Web Services, Inc. nor any of its Affiliates are a party to this Agreement and none of them will have any liability or obligations hereunder.

11.5. Amendment to the Data Processing Addendum. The Data Processing Addendum (DPA) attached to the Standard Contract is hereby amended to include the following additional information. For the avoidance of doubt, in the event any of the below provisions conflict with the DPA appended to the Standard Contract, the below provisions shall take precedence.

Licensor-Specific Data Protection/Processing Information and Privacy Policy

I. Licensor-Specific Data Protection and Data Processing Information

1.0 Roles of the Parties

1.1 Data Controller

For user account data: Licensor is the Data Controller

BC Platforms AG

Bleicherweg 10, 8002 Zürich, Switzerland.

For research datasets:
The relevant pharma sponsor or data partner is the Data Controller, unless otherwise agreed in writing.

1.2 Data Processors

Licensor subsidiaries and approved sub-processors may process data on behalf of the Data Controller, including hosting providers (e.g., AWS) and technical support personnel.

1.3 User Role

Users act as authorized individuals under the instructions of their employer or organization. Users must comply with this Agreement and any internal instructions provided.

2.0 Personal Data Processing

2.1 Categories of Data

The Product processes:

- user identification and account data;
- usage logs and audit trail information; and
- support information Buyer or Users voluntarily provide.

2.2 Purpose of Processing

Personal data is processed to:

- operate and secure the Product;
- authenticate users;
- provide support;
- meet regulatory and security requirements; and
- improve the Product.

2.3 Legal Basis

Depending on your organization's setup, processing may rely on:

- performance of a contract (Terms of Use or service agreement);
- legitimate interests (secure and functional Application); and/or
- compliance with regulatory requirements.

2.4 Rights of the User

Users may exercise rights of access, rectification, restriction, objection, and other GDPR/Swiss/APPI/UK-GDPR rights by contacting: **dpo@bcplatforms.com**.

2.5 HIPAA-Specific Roles

If PHI is ever processed, Licensor acts as a Business Associate and complies with the content of the Privacy Policy and the **HIPAA Business Associate Addendum for the Standard Contract for AWS Marketplace**, which is hereby incorporated by reference.

3.0 International Data Transfers

Where data is transferred internationally (e.g., to the US or Asia), appropriate transfer mechanisms are applied, including SCCs, the EU–US and Swiss–US DPF frameworks, and transfer impact assessments.

For further information on data processing within the Product, please see the Privacy Policy.

4.0 Data Security & Compliance

Licensor maintains an ISO 27001–certified Information Security Management System and uses industry-standard administrative, physical, and technical safeguards, including:

- access controls;
- encryption at rest and in transit;
- audit logging;
- secure cloud infrastructure; and
- incident response procedures.

5.0 Third-Party Services and Sub-processors

The Application uses carefully selected sub-processors for hosting, support, and system functionality. These providers operate under data protection agreements ensuring compliance.

A full list of sub-processors can be found in the Privacy Policy.

6.0 Contact Information

For questions about this Agreement or data processing, contact:

BC Platforms AG (Licensor)

Data Protection Officer
dpo@bcplatforms.com

II. Privacy Policy

1. PURPOSE

The purpose of this Privacy Policy is to explain how personal data is collected, used, stored, and protected within the Product. It ensures that all individuals using the Product understand the types of data processed, the reasons for processing, and the safeguards in place to protect privacy, security, and confidentiality.

This policy supports transparency, regulatory compliance, and trust by outlining:

- the categories of personal data handled by the Product,
- the legal bases and purposes for processing,
- the responsibilities of the parties involved,
- data sharing practices and international transfers,
- applicable retention periods,

- and the rights available to individuals under relevant privacy laws.

2. SCOPE

This Privacy Policy applies to all personal data processed within the Product, including data collected from platform users (such as authentication and usage information) and any pseudonymised or anonymised research datasets processed on behalf of clients and data partners. It covers all environments and components that form part of the Product, including analytics modules, secure workspaces, and integrated tools used to support platform functionality.

This Privacy Policy applies to personal data processed within the Product in relation to individuals who use the Product under contractual agreements.

This policy does not apply to:

- Licensor personnel who interact with the Product solely as necessary to perform support, maintenance, security monitoring, configuration, or operational tasks. Such internal access is governed exclusively by Licensors' internal employment, confidentiality, information security, and privacy policies, and is not subject to this externally-facing Privacy Policy.
- Systems or environments outside the Product (e.g., customer-managed installations, third party research systems used independently by clients).
- Data processing activities governed under separate project-specific agreements, Master Service Agreements (MSAs), Research or Site Agreements, unless specifically incorporated therein.
- Data processing performed by Buyer, Users, or data partners in their own systems after export or receipt of results.

4. DEFINITIONS

Administrator / Internal team
Licensor or its subcontractors' personnel with elevated permissions who access the Product for support, maintenance, troubleshooting, configuration, or security purposes. Their access is governed by internal employment, confidentiality, and information security policies.

Controller / Data Controller
The legal entity that determines the purposes and means of processing personal data within the Product. For platform user data, Licensor acts as the controller. For research datasets, the controller is generally the client or data partner supplying the data (e.g., a pharma company or hospital).

Processor / Data Processor
A legal entity processing personal data on behalf of the controller. Licensor and its subsidiaries may act as processors when handling client provided datasets.

Data Subject
A natural person whose personal data is processed. In the Product, this may refer to:

- End-users of the Product (e.g., researchers), or
- Patients whose pseudonymised health data is processed by the platform.

Personal Data

Any information relating to an identified or identifiable individual, including user account data, logs, behavioural analytics data, and pseudonymised health data (which remains personal data under GDPR, UK-GDPR, and Swiss privacy law).

Sensitive Personal Data / Special Categories of Data
Health-related or other protected data types as defined in GDPR Art. 9, Swiss DPA, and equivalent laws. In the context of the Product, this refers primarily to pseudonymised patient datasets used for research.

User
An individual authorised by Buyer to access and use the Product for research, analytics, or operational purposes. "Users" include external researchers, analysts, and other individuals operating the platform under a customer or partner agreement. Internal BC Platforms' employees are not considered "Users" for the purpose of this policy unless they use the platform in the same capacity as external users.

2. Third Party Providers

AWS is the cloud infrastructure provider for Licensor's Product. Licensor implements its applications and services using AWS-provided hardware for computing, processing and storage, and AWS–provided services for security, network configuration, and data storage management.

Licensor uses Pendo, a product analytics and user experience platform, to analyze how users interact with our application. Pendo collects usage data such as feature interactions, page views, device information, and session metadata to help us improve product usability and performance.

3. Data Protection Officer

Licensor has appointed a Data Protection Officer responsible for overseeing compliance with applicable data protection laws and for serving as the primary contact point for privacy related questions, concerns, or requests. The Data Protection Officer can be reached at:
Email: dpo@bcplatforms.com

Buyer and/or Users may contact the Data Protection Officer for any matters relating to the processing of their personal data or the exercise of their data subject rights.

4. Authorised Organisations

Authorised Organisations are entities such as pharmaceutical companies, hospitals, academic research institutions, or other partners that have been granted access to the Product for the purpose of analysing health datasets as part of approved research activities. Their access to datasets and analytical features is governed exclusively by the contractual Agreements concluded with Licensor.

Individual employees, analysts, or researchers acting on behalf of Buyer or another authorized organisation and logging into the Product are considered **Users** under this Privacy Policy and are subject to its provisions and the Terms of Use. However, the organisational entities themselves are not considered "Users" for the purposes of this Policy.

Authorised organisations can access only the datasets, analysis environments, and project spaces assigned to them under their agreements. Access to datasets of other organisations is not permitted unless explicitly agreed in writing between all relevant Data Controllers.

6. CATEGORIES OF PERSONAL DATA COLLECTED

Product User Data
The following categories of personal data may be processed about Users who log into and interact with the Product:

- **Identification and Account Data**:
  Name, work email address, organisation, role, login username, and account status.
- **Authentication and Security Data**:
  Login timestamps, session identifiers, multifactor authentication data (where applicable), and security event logs necessary to maintain platform integrity.
- **Usage and Activity Logs**:
  Records of actions performed within the Product (e.g., queries run, tools used, features accessed), captured for auditability, platform reliability, and compliance with security standards such as ISO 27001 and 21 CFR Part 11.
- **Support and Communication Data**:
  Information Users provide voluntarily in support tickets, feedback forms, or when contacting Licensor for assistance.
- **Behavioural Analytics Data**:
  Information about how Users interact with the Product, including page views, feature usage, session duration, and click paths. This data is used to understand User engagement and improve the Product. Users may object to such processing and may request deletion of their analytics data at any time.

7. REGULAR INFORMATION SOURCES

The Product does not receive personal data about Users from external regular information sources. All personal data covered by this Privacy Policy is provided directly by Users or generated through their use of the platform (e.g., authentication data, usage logs, and behavioural analytics).

8. PURPOSES OF PERSONAL DATA PROCESSING

The intended use cases of the personal data in the Product can be described as follows:

- **Provision and Improvement the Service:** Use of User account data and logs to authenticate Users, maintain the Product, provide customer support, and improve user experience.
- **Product Analytics and User Enablement:** Licensor uses behavioural analytics to understand how users interact with the Product, in order to help Licensor improve the Product, identify usage patterns, and categorise Users (e.g. “active” or “inactive”) to tailor communications and support. This may involve profiling as defined under GDPR Article 4(4), although it does not involve automated decision-making with legal or similarly significant effects. Users may object to this processing at any time, after which such analytics will no longer be collected for that User.
- **Regulatory and Security Requirements:** Monitor logins and actions (audit trails) for security, compliance with regulations (e.g., 21 CFR Part 11 audit requirements), and to investigate any improper access. These audit logs are essential for platform security and regulatory compliance.
- **Fulfilling Legal Obligations:** If applicable, ensure that Buyer meets legal obligations (e.g., complying with data protection laws, responding to lawful data access requests).

Only the **minimum necessary data** is used for each purpose, in line with data minimisation principles (GDPR Art.5(1)(c)).

9. LEGAL BASIS FOR PROCESSING AND COMPLIANCE FRAMEWORK

A. User Account, Authentication, and Service Provision

Processing of personal data such as identification details, account credentials, and essential usage information is carried out to authenticate Users, maintain access control, and ensure the functioning and support of the Product.

The legal basis for this processing is based on:

- **Contractual necessity** – to provide the services under the applicable agreement through which the User is authorised to access the Product; and
- **Legitimate interests** (GDPR Art. 6(1)(f) – in operating a secure, stable, and reliable Product, if Users' rights and freedoms are not overridden.

B. Usage Logs, Security Monitoring and Audit Trails

The Product automatically generates and processes operational data such as authentication events, access logs, audit trails, and security-relevant system activity. This processing is necessary to:

- maintain platform security,
- detect and investigate improper access or misuse,
- comply with audit and regulatory requirements (e.g., 21 CFR Part 11–style logging expectations), and
- support troubleshooting and service reliability.

The legal basis for this processing is **legitimate interests** (GDPR Art. 6(1)(f)), as Licensor has a strong and necessary interest in ensuring the security, integrity, and auditability of the Product in line with GDPR Art. 32, contractual obligations, and relevant regulatory expectations.

C. Behavioural Analytics

Behavioural analytics data is processed to understand how Users interact with the Product, improve usability, support product development, and tailor training or support.

The legal basis for this processing is legitimate interests (GDPR Art. 6(1)(f)).

Users have the right to object to this processing and may request deletion of their behavioural analytics data at any time.

10. DATA RECIPIENTS AND SHARING

Licensor may share User personal data only with the following categories of recipients:

A. Licensor subsidiaries acting as data processors, as listed in Section 5.2.

B. Approved technical processors, such as cloud hosting providers, authentication services, and product analytics tools (e.g., Pendo), engaged under appropriate contractual safeguards.

C. Regulatory or supervisory authorities, where required by applicable laws.

D. Other third parties only if required by law, or where expressly instructed by the User's employer or partner organisation under applicable contractual terms.

Licensor does not share User personal data with pharma companies, hospitals, or research partners for their independent use.

11. INTERNATIONAL DATA TRANSFERS

Data Residency
User data is stored in AWS Europe Frankfurt data centre.

Transfers Outside EU/Switzerland
If data needs to be processed in the US or other countries (for example, by internal or data processor team members in the US or India), we ensure lawful transfer mechanisms. This includes:

- For EEA -> US: compliance with the EU–US Data Privacy Framework (DPF) if applicable or using EU Standard Contractual Clauses (SCCs) with supplementary measures.
- For Switzerland -> US: likewise, the Swiss–US DPF or Swiss-approved SCCs are used.
- For EEA/Switzerland -> Japan: Japan is considered to have adequate data protection; additionally, safeguards required by APPI, GDPR and other privacy laws are in use in any data transfers.
- For EEA -> India: using EU Standard Contractual Clauses (SCCs) with supplementary measures.
- Conducting Transfer Impact Assessments (TIAs) where needed to evaluate cross-border data access risks.

No data transfers to countries without adequate protection will occur without these safeguards.

12. DATA RETENTION POLICY

User Account Data: Retained for as long as the User has an account on the Product and the Buyer relationship is active. Licensor may remove or anonymise user personal data within 6–12 months after a user leaves or the contract ends, unless needed for legal purposes.

Usage Logs & Audit Trails: Kept for a defined period, according to Product classification and any applicable Enterprise SLAs to support security investigations, compliance audits (such as verifying regulatory compliance), and service improvement. After this period, logs containing personal identifiers are deleted or anonymised.

Behavioural Data: Usage data collected is retained for as long as the User account is active. When a User’s Product account is deactivated or deleted, Licensor will ensure that their usage history and account details are also deleted in accordance with GDPR and Licensor’s internal data retention policies.

Backups: Note that data may reside in secure backups for a short additional period before deletion, per disaster recovery policies. These backups are protected with the same security measures until they expire.

No personal data is kept longer than necessary for the purposes defined, in accordance with the storage limitation principle. Once data is no longer needed, it is securely deleted.

13. RIGHTS AND CHOICES OF THE USER

The following data subject rights are available to users (and possibly to patients, if applicable) under GDPR and Swiss law:

- **Right of Access:** Individuals can request a copy of their personal data that we hold.
- **Right to Rectification:** Individuals may correct inaccurate personal data (e.g. update contact information).
- **Right to Erasure:** They can request deletion of personal data in certain circumstances – for instance, if they leave the company and wish their user account data removed, provided we have no overriding need to keep it, for example, for regulatory audit purposes.
- **Right to Restrict Processing:** Individuals can ask us to limit processing if they contest data accuracy or object to processing (where applicable).
- **Right to Object:** When Licensor processes data based on legitimate interests, Users can object to certain uses.
- **Right to Data Portability:** (Applicable mainly to user-provided data) Users may request to receive their data in a common format, where applicable.
- **Right to Lodge a Complaint:** Users are informed they can contact Licensor's DPO for issues and have the right to complain to a supervisory authority (e.g., an EU Data Protection Authority or the Swiss FDPIC) if they believe their data is mishandled.
- **Right to Object to Profiling:** Buyer or Users may object to the use of data for profiling purposes (e.g. categorisation into "active" or "inactive" users for communication tailoring). You may also request that your usage data collected be deleted.

How to Exercise Your Rights?
Buyer and/or Users may exercise their above stated rights by contacting the data controller by sending an email to the following e-mail address: dpo@bcplatforms.com. Licensor aspires to provide a reply as soon as possible and where needed, and provide additional instructions or ask additional questions based on the request.

Please note that prior to fulfilling a request, Licensor has a right as well as an obligation to verify the requestor's identity, due to which Licensor must be able to recognize you in an adequate manner.

14. PROFILING

The Product uses Pendo to analyse User behaviour and categorise Users (e.g. "active" or "inactive") to support Product development and User engagement. This constitutes profiling under GDPR Article 4(4). However, it does not involve automated decision-making that produces legal or similarly significant effects on individuals. Users may object to such profiling and request deletion of their usage data.

15. USE OF AI

User data is not processed by AI agents.

16. DATA SECURITY MEASURES

Licensor is an ISO 27001 certified company and follows the industry best practices in all its operations. The following technical and organizational measures are in place to protect data, assuring compliance with GDPR Art.32, Swiss DPA, 21 CFR Part11, and HIPAA security requirements:

- **Access Controls:** Only authorized Users can access the system. Users each have individual accounts; internal admins have separate, logged accounts. Role-based permissions ensure Users see only data they should.

- **Audit Logging:** The system maintains detailed audit logs of data access and User actions. Administrators can review who accessed what data and when, helping detect unauthorized activity.
- **Secure Infrastructure:** The cloud environment is managed under an ISO/IEC 27001-certified Information Security Management System (ISMS), with controls aligned to industry best practices and regularly audited by independent assessors. Regular penetration tests, vulnerability scanning, and security assessments are performed, and identified issues are remediated. The platform's application layer is designed and tested against the OWASP Application Security Verification Standard (OWASP ASVS), using its requirements as the baseline for secure development and verification.
- **Data Isolation:** Each Buyer's/User's data is logically separated. Different application instances do not share data resources or accounts. Within the Product itself, research projects are further isolated from each other to prevent cross-referencing of research cohorts. If Buyer/User data governance requires strict control over data copying (downloads and exports), a proxy system is available for configuration.
- **Employee Training & Policies:** All Licensor staff with access to data are trained in data protection and sign confidentiality agreements. There are internal policies (InfoSec, Privacy SOPs) that employees must follow. Licensor has an Information Security Management System (ISMS) and Privacy Information Management System (PIMS), indicating systematic protection of data.
- **Contingency Plans:** Backups, disaster recovery, and incident response plans are in place for Licensor and the Product. In case of any incident, Licensor can recover data and will notify relevant parties as required by the applicable law and/or customer and/or data partner agreements.

17. UPDATES TO THIS POLICY

Licensor may update this policy from time to time, for example, if regulatory requirements change or new features affect personal data use. Licensor will notify Buyer/Users of any significant changes. The latest version will always be accessible in the Product.

18. CONTACT INFORMATION AND FURTHER QUESTIONS

If you have any questions about this privacy policy or your data, please contact Licensor's Data Protection Officer at dpo@bcplatforms.com. We encourage you to reach out for any concerns, questions or recommendations.

12. **Reaffirmation of Obligations.** The Parties expressly reaffirm their obligations pursuant to the Standard Contract and the Agreement.

13. **No Other Changes.** Except as expressly modified by this Amendment, all terms of the Standard Contract and the Agreement remain in full force and effect.

This Amendment is effective contemporaneously with the Parties' acceptance of the Standard Contract, their entry into the Agreement, and the Subscription purchase.

HIPAA Business Associate Addendum for the Standard Contract for AWS Marketplace

This HIPAA Business Associate Addendum (this **"BAA")** is part of the Standard Contract for AWS Marketplace (the **"Standard Contract")** between Buyer and Licensor and governs the creation, receipt, maintenance, or transmission of Protected Health Information on behalf of the Covered Entity (the "**Buyer**") by the Licensor as Business Associate (the "**Supplier**"). Each of the Standard Contract and/or the Data Subscription Agreement is a Standard Contract. Each Seller and each Licensor is a Supplier. This Addendum is not applicable if Supplier does not create, receive, maintain, or transmit Protected Health Information on behalf of Buyer or if Buyer is not subject to the Administrative Simplification of the Health Insurance Portability and Accountability Act of 1996, as amended, the Health Information Technology for Economic and Clinical Health Act of 2009, and their implementing regulations (collectively **"HIPAA")** as a Covered Entity or Business Associate.

1. Definitions

1.1 All capitalized terms used but not otherwise defined in this BAA or the Standard Contract shall have the same meaning as those terms are defined by HIPAA.

1.2 "**Individual**" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.3 "**Protected Health Information**" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, and refer to individually identifiable information that is received, created, maintained, or transmitted by Supplier on behalf of Buyer.

2. Permitted Uses and Disclosures by Supplier

2.1 Except as otherwise limited in this BAA, Supplier may Use or Disclose Protected Health Information in its possession to perform functions, activities, or services for, or on behalf of, Buyer as specified in the Standard Contract consistent with Buyer's minimum necessary policies and procedures, provided that such Use or Disclosure would not violate HIPAA if done by Buyer.

2.2 Except as otherwise limited in this BAA, Supplier may Use Protected Health Information for the proper management and administration of Supplier or to carry out the legal responsibilities of Supplier.

2.3 Except as otherwise limited in this BAA, Supplier may Disclose the Protected Health Information in its possession to a third party for the proper management and administration or to fulfill any legal responsibilities of Supplier, provided that:

2.3.1 The Disclosure is Required by Law; or

2.3.2 Supplier has received from the third party reasonable written assurances that: (1) the information will remain confidential and will be Used or further Disclosed only as

Required by Law or for the purpose for which it was Disclosed to the party; and (2) the third party will notify Supplier of any instances of which it becomes aware in which the confidentiality of the information has been breached.

2.4 Supplier may not Use Protected Health Information to create de-identified Health Information in accordance with 45 C.F.R. § 164.514(b) for purposes unrelated to the Standard Contract without prior written approval of Buyer.

3. Obligations and Activities of Supplier

3.1 Supplier shall not Use or Disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law.

3.2 Supplier agrees to use appropriate administrative, physical, and technical safeguards and comply, where applicable, with the Security Standards for Protection of Electronic Protected Health Information, 45 C.F.R. Part 164 Subpart C (the "**Security Rule**") with respect to Electronic Protected Health Information, to prevent Use or Disclosure of the Protected Health Information other than as provided for by this BAA.

3.3 Supplier agrees to comply with the applicable requirements of the Security Rule.

3.4 Supplier agrees to mitigate, to the extent practicable, any harmful effect that is known to Supplier of a Use or Disclosure of Protected Health Information by Supplier in violation of the requirements of this BAA.

3.5 Supplier agrees to report to Buyer, without unreasonable delay and no later than within five (5) business days of discovery:

3.5.1 Any Use or Disclosure of Protected Health Information not provided for by this BAA, including Breaches of Unsecured Protected Health Information; and/or

3.5.2 Any Security Incident, provided that this Section shall hereby serve as notice, and no additional reporting shall be required, of any unsuccessful attempts at unauthorized Access, Use, Disclosure, modification, or destruction of information or unsuccessful interference with system operations in an information system.

3.6 For any Breach of Unsecured Protected Health Information of which it becomes aware, Supplier agrees to supplement the above report with the information required by 45 C.F.R. § 164.410 without unreasonable delay and in no case later than 30 calendar days after discovery of the Breach.

3.7 In accordance with 45 C.F.R.§ 164.502(e)(1)(ii) and 164.608(b)(2), Supplier agrees to ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on Supplier's behalf agree in writing to: (a) the same restrictions and conditions that apply through this BAA to Supplier with respect to such Protected Health Information and meet HIPAA requirements, including complying with the applicable requirements of the Security Rule; and (b) comply with the requirements of the Security Rule that apply to a Business Associate. Supplier shall not allow any of its Subcontractors to create, receive, maintain, or transmit Protected Health Information on Supplier's behalf unless Supplier first has conducted reasonable due diligence of the Subcontractor and its information security and determined that its security is reasonable.

3.8 Supplier agrees to make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information received from, or created or received by Supplier on behalf of Buyer, available to the Secretary of the Department of Health and Human Services ("**Secretary**") for the purposes of the Secretary determining compliance with HIPAA. Nothing in this Section shall be construed as a waiver of any legal privilege or of any protections for trade secrets or confidential commercial information.

3.9 Supplier, upon request by Buyer, will make Protected Health Information in a Designated Record Set available to Buyer or, at the request of Buyer, the Individual, within five (5) days of Buyer's request, as necessary to allow Buyer to comply with its obligations to provide access to Individuals of their health information as required by 45 C.F.R. § 164.524. To the extent that Protected Health Information in a Designated Record Set is available to Buyer through access to the SaaS Service, then Supplier satisfies its obligations under this Section through the provision of the SaaS Service.

3.10 Supplier, upon request by Buyer, will make Protected Health Information in a Designated Record Set available to Buyer and will incorporate any amendments to such information as instructed by Buyer within ten (10) days of a request, as necessary to allow Buyer to comply with its amendment obligations as required by 45 C.F.R. § 164.526. To the extent that Buyer can amend Protected Health Information in a Designated Record Set through use of the SaaS Service, then Supplier satisfies its obligations under this Section through the provision of the SaaS Service.

3.11 Supplier will maintain and, upon request by Buyer, within ten (10) days provide Buyer with the information necessary for Buyer to provide an Individual with an accounting of Disclosures as required by 45 C.F.R. § 164.528.

3.12 To the extent that Supplier is to carry out one or more of Buyer's obligations under the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164 Subpart E (the "**Privacy Rule**"), including but not limited to the provision of a notice of privacy practices on behalf of Buyer, Supplier shall comply with the requirements of the Privacy Rule that apply to Buyer in the performance of such obligations.

4. Obligations of Buyer

4.1 In the event that Buyer is a Covered Entity, then Buyer shall notify Supplier of any limitation(s) in Buyer's notice of privacy practices under 45 C.F.R. §164.520, to the extent that such limitation may affect Supplier's use or disclosure of Protected Health Information. In the event that Buyer is purchasing the SaaS Services as a Business Associate of one or more Covered Entities, then Buyer shall notify Supplier of any applicable limitation(s) of a Covered Entity's notice of privacy practices under 45 C.F.R. §164.520, to the extent that Buyer is aware of such limitation and such limitations may affect Supplier's use or disclosure of Protected Health Information.

4.2 Buyer shall notify Supplier of any changes in, or revocation of, the permission by an Individual to use or disclose his or her Protected Health Information, to the extent that Buyer is aware of such changes and such changes may affect Supplier's use or disclosure of Protected Health Information.

4.3 Buyer shall notify Supplier of any restriction on the use or disclosure of Protected Health Information under 45 C.F.R. §164.522, to the extent that Buyer is aware of such restriction and such restriction may affect Supplier's use or disclosure of Protected Health Information.

4.4 Buyer shall not knowingly request or cause Supplier to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Buyer, except as otherwise set forth in Sections 2.2 and 2.3 of this BAA.

5. Term and Termination

5.1 This BAA shall remain in full force and effect through the term of the Standard Contract.

5.2 For purposes of the termination provisions of the Standard Contract at Section **10.2** of the Standard Contract, a breach of this BAA shall constitute a breach of the Standard Contract.

5.3 Except as provided in Section 5.4 of this BAA, upon termination of the Standard Contract for any reason, Supplier shall return or destroy all Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of Subcontractors of Supplier. Supplier shall retain no copies of the Protected Health Information.

5.4 In the event that Supplier determines that returning or destroying the Protected Health Information is infeasible, and to the extent the Supplier retains any knowledge of the Protected Health Information, then Supplier shall extend the protections of this BAA to such Protected Health Information and limit further Uses and Disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for as long as Supplier maintains such Protected Health Information. This Section shall survive the termination of this BAA for any reason.

6. Miscellaneous

6.1 This BAA modifies and supplements the terms and conditions of the Standard Contract and shall be deemed a part of the Standard Contract. Any ambiguity in this BAA shall be resolved to permit the parties to comply with HIPAA and other applicable laws. In the event any provision of the Standard Contract conflicts or is inconsistent with this BAA, then this BAA shall control.

6.2 Nothing in this BAA shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

6.3 Except as specifically required to implement the purposes of this BAA, or to the extent inconsistent with this BAA, all other terms of the Standard Contract shall remain in force and effect.