HIPAA BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (**"Business Associate Agreement" or "BAA"**) is made as of the later signing date below ("**Effective Date** "), by and between **CyberArk Software, Inc.**, a Delaware corporation having its principal place of business at 60 Wells Avenue, Newton, MA 02459 and the customer entity specified on the signature line below (or if this BAA is being incorporated by reference, the customer entity party to the Agreement) ("**Customer**").

This Business Associate Agreement is entered into between CyberArk and Customer in order to implement compliance with the requirements of HIPAA. This BAA amends and is a part of the Terms of Service, or other written agreement governing CyberArk's provision of software-as-a-service ("**SaaS**") products to Customer, between CyberArk and Customer ("**Services Agreement**"); and

WHEREAS, CyberArk provides a SaaS solution and other Services to Customer, and CyberArk does not always know the particular details of the content of information provided by Customer, or whether it may contain Protected Health Information (as defined below).; and

WHEREAS, the parties desire to enter into this BAA as set forth below so that if CyberArk receives PHI from CyberArk Product Users of the Service and maintains or processes the PHI on behalf of the Customer, this BAA will address the obligations of the parties relative to the Privacy Rule, the Security Rule,and the Breach Notification Rule, all as defined further below.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of whichis hereby acknowledged, CyberArk and Customer agree as follows:

1. Obligations of CyberArk. The parties hereby agree that the terms of this BAA will only apply if Customer is a Covered Entity or Business Associate and Customer or Customer Users create, receive, maintain, or transmit PHI as part of the Services such that CyberArk is deemed to be acting as Customer's Business Associate, or a subcontractor of a Business Associate. The parties hereby further agree that this BAA does not apply: (a) to any other CyberArk Product, service, or feature not part of a Service; (b) to any data other than PHI that may be disclosed to CyberArk pursuant to the Services or; (c) in any other manner from a geography other than the United States.

1.1. Use and Disclosure. CyberArk may only use or disclose PHI: (a) as set forth in this BAA and to perform the Services, (b) for the proper management and administration of CyberArk's business, or (c) where required by law and to carry out the legal responsibilities of CyberArk, including to enable judicial or administrative proceedings and law enforcement purposes. CyberArk will not use or further disclose the information other than as permitted or required by this BAA or as required by law

CyberArk agrees to make reasonable efforts to limit the use and disclosure of and requests for PHI to the minimum necessary to accomplish the intended purposes of the use, disclosure, or request and shall not use or disclose PHI in a manner that would violate the Privacy Rule if done by Customer.

Any permitted disclosure of PHI by CyberArk to a third party will either be required by law or subject to reasonable assurances obtained by CyberArk from the third party that PHI will be held in a manner consistent with the restrictions and conditions set forth in this BAA, and used or disclosed only as required by law or for the purposes for which it was disclosed to such third party, and that any Breach of confidentiality of PHI which become known to such third party will be reported to CyberArk.

1.2. De-Identified Information and Data Aggregation. CyberArk may aggregate data and use data for its reasonable business purposes where CyberArk has sufficiently de-identified the data in

compliance with HIPAA, pursuant to 45 C.F.R. §164.514(b).

1.3. Safeguards. As applicable, CyberArk shall use safeguards that are appropriate and commercially reasonable to prevent use or disclosure of PHI other than as permitted or required by this BAA or the Agreement, in accordance with the requirements under applicable federal and state laws, including the HIPAA Security Rule. Further, as applicable and as required by the Security Rule, CyberArk shall comply with 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314 and 164.316 of the Security Rule and implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information. CyberArk has no obligation to protect PHI under this BAA to the extent Customer creates, receives, maintains, or transmits such PHI outside of the Services.

1.4. Privacy Rule. Customer has not assigned any Customer obligations under the Privacy Rule to CyberArk other than as may be explicitly set forth in this BAA.

1.5. Agents and Subcontractors. Consistent with the second paragraph of Section 1.1 of this BAA, CyberArk will take appropriate measures to ensure that any agents and subcontractors to whom it provides access to PHI on behalf of CyberArk, agree in writing to obligations that provide the same material level of protection of PHI as CyberArk is required to provide under this BAA.

1.6. Designated Record Set. Customer agrees that CyberArk does not have, nor does it maintain PHI or other health information that is part of the Designated Record Set maintained by Customer. Moreover, Customer acknowledges that Customer has not requested pursuant to this BAA or the Agreement and will not request that CyberArk maintain or in any way be responsible for any part of a Designated Record Set of Customer. Except to render the PHI or ePHI de-identified as may be permitted under this BAA, CyberArk will not amend, supplement, or delete any part of, revise or otherwise alter the Protected Health Information that may be maintained by CyberArk pursuant to the Services, such that any PHI maintained by CyberArk will be a subset of the PHI maintained by the Customer.

1.7. Requests/Rights of Individuals with Respect to PHI. If CyberArk receives any request from an individual with respect to PHI, including, without limitation, a request for access, amendment, erasure, restrictions on use or disclosure, request for accommodation for confidential communications, or an accounting of disclosures, CyberArk shall promptly forward such requestto Customer, to the extent the individual submitting the request identifies the Customer as the source of the PHI. Following receipt of such notice from CyberArk, Customer shall be solely responsible for responding to such request and shall not request CyberArk's assistance with such request. Customer acknowledges that as part of its commitment to privacy, CyberArk maintains PHI in a manner that does not usually and reasonably permit CyberArk to associate the PHI with an individual nor generally with the Customer and Customer further acknowledges and agrees that requests from individuals, including those set forth in this Section of the BAA, are not an obligation or a responsibility of CyberArk under this BAA, the Services Agreement, or any other document or law. Thus, any request from an individual must identify Customer for CyberArk to make such connection to the Customer and notify Customer of the request. Otherwise, if the individual does not or cannot identify the Customer, CyberArk will inform the individual making the request that they need to contact their health care provider directly to exercise such rights.

1.8. Audit. Where applicable, CyberArk shall make its internal practices, books, and records relating to the use and disclosure of PHI, received from Users or Customer, available to the Secretary of Health and Human Services, upon request, for purposes of determining and facilitating CyberArk's and/or Customer's compliance with HIPAA.

1.9. Reporting of Breach of Unsecured PHI. Upon CyberArk's discovery of a Security Incident that impacts Customer PHI or discovery of a Breach of Unsecured PHI by CyberArk or its sub-contractors, and after reasonable inquiry to determine the scope and to apply reasonable mitigations, CyberArk will notify Customer without unreasonable delay and in no case later than 60 days from

the discovery of the Security Incident or Breach of Unsecured PHI as permitted by HIPAA, and in a manner and timing that is consistent with the needs of any law enforcement authority and applicable law. The notice shall, to the extent reasonably feasible, include the identity of each Individual whose Unsecured PHI was involved in the Breach and a brief description of the Breach, although Customer understands and acknowledges that, given the nature of the Services, identification of an individual associated with any such PHI is very unlikely.

Notwithstanding the above, this Section will also function as CyberArk's notice to Customer that CyberArk periodically experiences unsuccessful attempts to gain unauthorized access, use, disclosure, modification, or destruction of information, as well as unsuccessful attempts to generally disrupt the operation of CyberArk's information systems, including the Services. CyberArk further hereby provides notice to Customer that even if such attempts and events constitute a Security Incident as that term is defined under HIPAA, CyberArk will not provide any further notice to Customer regarding such unsuccessful attempts and events.

1.10. Mitigation. CyberArk shall, to the extent practicable, provide Customer with information about any actions that have been taken by Business Associate to mitigate any effects of the Breach. CyberArk will take reasonable measures to mitigate, to the extent practicable, any harmful effect of a Breach that is known to CyberArk.

2. Obligations of the Customer. Customer agrees that:

2.1. Where the compliance with a requirement of this BAA requires actual knowledge by CyberArk as to whether Protected Health Information is involved, Customer shall advise CyberArk regarding PHI content, and any other details regarding such PHI necessary for CyberArk's performance of this BAA.

2.2. Customer has included, and will include, in its Notice of Privacy Practices a statement that Customer may disclose PHI for treatment, payment, health care operations purposes and any other purpose which relates to Services provided by CyberArk to Customer. Customer shall notify CyberArk of any limitation(s) in Customer's Notice of Privacy Practices agreed to in accordance with 45 C.F.R. § 164.520(b)(2), to the extent that such limitation(s) may affect CyberArk's use or disclosure of PHI.

2.3. Customer will not request CyberArk to use Protected Health Information in any manner that violates the Privacy Rule, or that would violate the Privacy Rule if so used by Customer (except for the purposes specified under 45 CFR § 164.504(e)(2)(i)(A) and (B)).

2.4. Customer represents and warrants that it will disable or not use any functionality on CyberArk Products other than the Services that would otherwise disclose PHI to CyberArk, and will instruct its Users to do the same.

2.5. Notwithstanding Customer's obligation to address all requests from individuals solely on its own and without assistance from CyberArk, including any obligations of Customer that followsuch requests, if Customer nonetheless believes that a specific request from an individual may change or affect CyberArk's ability to provide Services or to use or disclose PHI as set forthin this BAA, Customer shall promptly notify CyberArk in writing and Customer will take reasonable actions as requested by CyberArk, including possibly terminating this BAA or altering the Services, to assist CyberArk in complying with such request.

2.6. Customer, not CyberArk, is responsible for managing and determining in each instance whether Customer's Users are authorized to use the Services and to use and disclose PHI pursuant to such Services and CyberArk will have no obligations under this BAA related to such management and determinations.

3. Termination.

3.1. Termination for Failure to Comply. Upon learning of a violation of a material term of the BAA by the other party, the non-breaching party shall provide an opportunity for the breaching party to cure the material breach. If the breaching party does not cure the material breach within thirty (30) days, following the breaching party's receipt of written notice setting forth the details of such material breach, then the non-breaching party shall have the right to terminate this BAA and the Agreement. If termination is not feasible, the non-breaching party may report the problem to the Secretary or any other competent authority.

3.2. Automatic Termination. This BAA will terminate automatically upon termination or expiration of all any Agreement between the parties.

3.3. Termination for Change of Status. CyberArk may terminate this BAA if facts, circumstances, or law change in such a way as to render this BAA legally or factually unnecessary.If CyberArk terminates this BAA pursuant to this subsection, it shall give Customer notice of termination that includes the reasons for such termination.

3.4. Duties Upon Termination. Except as set forth herein and to the extent required to beretained by government regulations, upon termination, CyberArk shall return or destroy all confidential information as set forth in the Agreement. However, given the nature of the Services that CyberArk provides and the manner in which CyberArk protects the privacy and security of the Users of its Services, CyberArk has determined that destruction of all copies of PHI that it may maintain is infeasible. Therefore, after termination of the Services and pursuant to 45 CFR § 164.504(e)(2)(ii)(J), this BAA shall remain in effect and CyberArk shall continue to observe its obligations under this BAA to the extent copies of the PHI are retained by CyberArk and shall limit further uses and disclosures of PHI to the purposes that make its return or destruction infeasible and that are consistent with the Privacy Rule.

4. Amendment. The parties shall amend this BAA from time to time by mutual written agreement to keep this BAA consistent with any changes made to the HIPAA laws or regulations in effect as of the date of this BAA and with any new regulations promulgated under HIPAA. Either party may terminate the BAA in whole or in part if the parties are unable to agree to such changes by the compliance date for such new or revised HIPAA laws or regulations.

5. No Third-Party Benefit. This BAA is for the sole benefit of the parties hereto and shall not confer or be deemed to confer any rights, benefits or claims upon any person or entity not a party to thisBAA.

6. Entire Agreement. This BAA, including any appendices, schedules or other exhibits now or subsequently attached hereto, constitutes the entire agreement between the parties with respect to the subject matter hereof.

7. Interpretation. In the event of any conflict between the provisions of this BAA and the Agreement, the provisions of this BAA shall control. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits the parties to comply with HIPAA.

8. Counterparts. This BAA may be executed in two or more counterparts, each of which shall be an original, but all of which taken together shall constitute one and the same agreement.

9. Indemnification. The parties' indemnification obligations shall be controlled by the Services Agreement or, in the absence of such a provision in the Services Agreement, the following will apply: (a) in no event will either party's maximum aggregate liability arising out of or related to the Services Agreement or this BAA exceed the total amount paid or payable to CyberArk under the Services Agreement during the twelve (12) month period preceding the date of initial claim, and (b) neither party will have any liability to the other party for any loss of profits or revenues, loss of goodwill, loss or

corruption of data or for any indirect, special, incidental, consequential or punitive damages arising out of, or in connection with the Services Agreement or this BAA.

10. **Governing Law**. This BAA shall be governed by the laws of the State of Massachusetts, notwithstanding any conflicts of law provisions to the contrary.

11. **Definitions**. Any capitalized terms not herein defined will have the meaning given to them in the Agreement, or if not defined in either this BAA or the Agreement, then they will have the meaning given to them in HIPAA.

11.1. "**Breach**" when capitalized, shall have the meaning set forth in 45 CFR § 164.402 (including all of its subsections); with respect to all other uses of the word "breach" in this BAA, the word shall have its ordinary contract meaning.

11.2. "**Breach Notification Rule**" shall mean the Standards for Breach Notification forUnsecured Protected Health Information, 45 CFR Part 164, Subpart D.

11.3. "**CyberArk Products**" shall mean all software, services, and products offered by CyberArk or its affiliates.

11.4. "**Electronic Protected Health Information**" or **"e PHI"** shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to the information created or received by CyberArk from or on behalf of Customer.

11.5. **"HIPAA"** means, collectively, the Health Insurance Portability and Accountability Act of 1996 and regulations thereunder, as amended and supplemented by the Health Information Technology for Economic and Clinical Health Act (HITECH) enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, all as amended.

11.6. "**Privacy Rule**" shall mean the Standards for Privacy of Individually Identifiable Health Information, 45 CFR Part 160 and Part 164.

11.7. "**Protected Health Information**" or "**PHI**" shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information created or receivedby CyberArk from or on behalf of Customer.

11.8. "**Security Rule"** shall mean the Security Standards for the Protection of Electronic Health Information , 45 CFR Part 160 and Part 164.

11.9. "**Services**" shall mean the CyberArk Services listed at https://www.cyberark.com/trust/hipaa-compliance/ and related support services, including the provision of updated, new, and related versions of the foregoing products and services as deemed appropriate by CyberArk.

11.10. "**Unsecured Protected Health Information**" or "**Unsecured PHI**" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402, limited to the information createdor received by CyberArk from or on behalf of Customer.

11.11. **"User" or "CyberArk Product User"** shall mean the individual employee, agent, consultant, contractor, or vendor authorized by Customer to use the CyberArk Product solely for the internal use of Customer and its Affiliates subject to the terms and conditions of the Agreement.

IN WITNESS WHEREOF, the parties have executed this Business Associate Agreement as of the Effective Date.

CyberArk	**Customer**
By: _____	By: _____
Title: _____	Title: _____
Company Name: _____	Company Name: _____
Date: _____	Date: _____