SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM: 18.3
(ID # 27947)
MEETING DATE:
Tuesday, June 10, 2025

FROM : RUHS-MEDICAL CENTER

SUBJECT: RIVERSIDE UNIVERSITY HEALTH SYSTEM - MEDICAL CENTER: Approve the SaaS Terms of Service Agreement with CyberArk Software, Inc., for Software and Cloud Services for one (1) year effective upon signature, All Districts. [Total Cost $260,855; up to $26,085 in Additional Compensation] 100% Hospital Enterprise Fund 40050

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve the SaaS Terms of Services Agreement (Agreement) with CyberArk, for Software and Cloud Services for one (1) year effective upon signature, for a total cost of $260,855 and authorize the Chair of the Board to sign the Agreement on behalf of the County; and
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459 and based on the availability of fiscal funding and as approved as to form by County Counsel, to: (a) sign amendments including modifications to the statement of work that stay within the intent of the Agreement and (b) sign amendments to the compensation provisions that do not exceed the total sum of ten percent (10%) of the total cost of the Agreement.
3. Authorize the Purchasing Agent to issue Purchase Orders for goods and or/services related to the Agreement that do not exceed the sum total of the total aggregate amount.

ACTION:Policy

Jennifer Cruikshank
Jennifer Cruikshank, Chief Executive Officer – Health System 5/27/2025

MINUTES OF THE GOVERNING BOARD

On motion of Supervisor Gutierrez, seconded by Supervisor Washington and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes:	Medina, Spiegel, Washington, Perez and Gutierrez
Nays:	None
Absent:	None
Date:	June 10, 2025
xc:	RUHS-MC

Kimberly A. Rector
Clerk of the Board
By: _____ Deputy

SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD OF DIRECTORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$260,855	$0	$0	$0
NET COUNTY COST	$0	$0	$0	$0
SOURCE OF FUNDS: 100% Hospital Enterprise Fund - 40050			Budget Adjustment: No	
			For Fiscal Year: 24/25	

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

The proposed action requests approval of a Software as a Service (SaaS) Terms of Service Agreement with CyberArk Software, Inc. (CyberArk), for the implementation of Privileged Identity Management (PIM) and Privileged Access Management (PAM) solutions, in response to the growing cybersecurity threats facing healthcare organizations.

The CyberArk solution satisfies the specific requirements of Riverside University Health System – Medical Center (RUHS-MC). By deploying this solution, Riverside University Health System – Information Technology (RUHS-IT) will be better equipped to mitigate risks associated with privileged access, ensure compliance with regulatory standards, and enhance operational efficiency.

Approval of this software request will help strengthen RUHS-MC against security vulnerabilities, enhance adaptability to compliance standards, streamlining access management processes to enhance productivity and performance. Strengthening and addressing these areas presents an opportunity to reduce operational costs, system downtime, reduced scalability, and slower incident response. Implementing a comprehensive, centralized access management solution will enhance security integrity and operational resistance while reducing the likelihood of security-related disruptions while supporting patient care at RUHS-MC and affiliated departments.

If Board of Supervisors approval is granted, RUHS-MC seeks to leverage cooperative agreement number AR2472 between NASPO ValuePoint and Carahsoft Technology Corporation. NASPO is a cooperative purchasing agency that is available to all government and educational entities and competitively solicited this agreement using the Request for Proposal (RFP) method by means of solicitation number CH16012. Through this solicitation it was determined that Carahsoft Technology Corporation is the most qualified and responsive bidder as Reseller of Software and Cloud services.

Impact on Residents and Businesses

These services are a component of RUHS-MC's system of care aimed at improving the health and safety of its patients and the community.

Contract History and Price Reasonableness

The Agreement that was leveraged between NASPO ValuePoint and Carahsoft Technology Corporation, Contract Number AR2472, has been competitively bid out utilizing the Request for Proposal (RFP) method of procurement. This agreement was entered into on October 14, 2016 and is effective through September 15, 2026.

An Addendum (NO. 7-17-70-40-05) to this Master Agreement was executed on September 15, 2017, to include all California political subdivisions/local governments. This Addendum provides the State of California with the same services and prices equal to or lower than those provided within the NASPO ValuePoint Master Agreement.

Amendment NO. 1 to the Addendum, executed on May 1, 2018, revised Section 9 of the Addendum, to include additional terms regarding orders placed with Carahsoft.

Amendment NO. 2 to the Addendum, executed on August 11, 2011, added additional products and services under the Addendum. These additional products and services included Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), along with the terms and conditions governing these additions.

Amendment NO.3 to the Addendum, executed on June 29, 2023, amended the Pricing section of the Addendum.

Amendment NO.4 to the Addendum, executed on December 20, 2024, added Generative Artificial Intelligence Reporting language to the Addendum.

This Agreement requires Board approval as the compensation provision exceeds the Purchasing Agent's authority and $100,000 threshold for contracting with a vendor for professional services per Purchasing Policy Manual, County Ordinance 459 and California Government Code § 25502.5.

ATTACHMENTS:

Attachment A: Software as a Service (SaaS) Agreement with CyberArk (Software and Cloud Services).
Attachment B: Business Associate Agreement with CyberArk
Attachment C: Scoping Letter with Carahsoft Technology Corporation (Distributor) through Glass Box Technology Inc (Reseller)

SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD OF DIRECTORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

Melissa Curtis
Melissa Curtis, Deputy Director of Purchasing and Fleet 5/23/2025

Jacqueline Ruiz
Jacqueline Ruiz, Principal Analyst 6/4/2025

Gregg Gu
Gregg Gu, Chief Deputy County Counsel 5/27/2025

SAAS TERMS OF SERVICE

CYBERARK SOFTWARE LTD. AND/OR ITS AFFILIATES ("**CYBERARK**") IS WILLING TO GRANT ACCESS TO THE SAAS PRODUCTS TO YOU AS THE COMPANY OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SAAS PRODUCTS (REFERENCED BELOW AS "**CUSTOMER**") ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS AGREEMENT (AS DEFINED BELOW). BY ENTERING INTO THIS AGREEMENT ON BEHALF OF THE CUSTOMER, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE CUSTOMER TO THIS AGREEMENT. CUSTOMER AND CYBERARK MAY EACH ALSO BE REFERRED TO AS A "PARTY" AND TOGETHER, THE "PARTIES".

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SAAS PRODUCTS. THIS SAAS TERMS OF SERVICE ("**AGREEMENT**") CONSTITUTES A LEGAL AND ENFORCEABLE CONTRACT BETWEEN CUSTOMER AND CYBERARK. BY INDICATING CONSENT ELECTRONICALLY, OR ACCESSING OR OTHERWISE USING THE SAAS PRODUCTS, CUSTOMER AGREES TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE TO THIS AGREEMENT, DO NOT INDICATE CONSENT ELECTRONICALLY AND MAKE NO FURTHER USE OF THE SAAS PRODUCTS.

1. Access and Use

1.1 **Access and Use.** CyberArk grants Customer, during the Subscription Term, a non-exclusive, non- transferable right to access and use (and permit Authorized Users of Customer and its Affiliates' to access and use) the SaaS Products and applicable Documentation solely for Customer's and its Affiliates' internal business purposes in accordance with the Documentation and in the quantity specified in the applicable Order. Such license grant is subject to payment of all applicable fees set forth in the Order or payment in accordance with an Indirect Order through a Channel Partner (as appropriate) and the terms and conditions of this Agreement. CyberArk may update or upgrade the SaaS Products from time-to-time.

1.2 **Access and Use Restrictions.** Customer shall not (directly or indirectly): (a) copy or reproduce the SaaS Products or the Documentation except as permitted under this Agreement; (b) exceed the subscribed quantities, Authorized users or other entitlement measures of the SaaS Products as set forth in the applicable Order; (c) remove or destroy any copyright, trademark or other proprietary marking or legends placed on or contained in the SaaS Products, Documentation or CyberArk Intellectual Property; (d) assign, sell, sublicense, distribute or otherwise transfer or make available the rights granted to Customer under this Agreement to any third party except as expressly set forth herein; (e) modify, reverse engineer or disassemble the SaaS Products; (f) except to the limited extent applicable laws specifically prohibit such restriction, decompile, attempt to derive the source code or underlying ideas or algorithms of any part of the SaaS Products, attempt to recreate the SaaS Products or use the SaaS Products for any competitive or benchmark purposes; (g) create, translate or otherwise prepare derivative works based upon the SaaS Products, Documentation or CyberArk Intellectual Property; (h) interfere with or disrupt the integrity or performance of the SaaS Products; (i) attempt to gain unauthorized access to the SaaS Products or its related systems or networks, or perform unauthorized penetrating testing on the SaaS Products; (j) use the SaaS Products in a manner that infringes on the Intellectual Property rights, publicity rights, or privacy rights of any third party, or to store or transfer defamatory, trade libelous or otherwise unlawful data; or (k) except as otherwise agreed by the Parties in the applicable BAA, store in or process with the SaaS Products any personal health data, credit card data, personal financial data or other such sensitive regulated data not required by the Documentation, or any Customer Data that is subject to the International Traffic in Arms Regulations maintained by the United States Department of State. Fees for the SaaS Products are based on use of the SaaS Products in a manner consistent with the Documentation. If Customer uses, or is reasonably suspected of using, the SaaS Products in violation of the Documentation or exceeding the licensed quantities or other entitlement measures as set forth in an applicable Order, Customer shall cooperate with CyberArk to resolve any non-compliance, which may include payment for any such overages at then-current applicable rates.

1.3 **Login Access to the SaaS Products.** Customer is solely responsible for ensuring: (i) that only appropriate Authorized Users have access to the SaaS Products, (ii) that such Authorized Users have been trained in proper use of the SaaS Products, and (iii) proper usage of passwords, tokens and access procedures with respect to logging into the SaaS Products. CyberArk may refuse registration of or suspend Customer's or a specific user's access and use of the SaaS Products if CyberArk knows or reasonably suspects that Customer's access or use is malicious or otherwise harmful to the Customer itself, the SaaS Products or CyberArk's other customers. CyberArk will provide notice prior to such suspension if permitted by applicable law and unless CyberArk reasonably believes that providing such

JUN 10 2025 18.3

notice poses a risk to the security of the SaaS Products. CyberArk will promptly reinstate Customer's access and use once the issue has been resolved.

1.4 **Trial Services**. If Customer is using a free trial, a proof of concept version of the SaaS Products, a beta version of the SaaS Products, or using the SaaS Products on any other free-of-charge basis as specified in an Order including any related support services to the extent provided by CyberArk in its sole discretion (collectively, "Trial Services"), CyberArk makes such Trial Services available to Customer until the earlier of: (i) the end of the free trial or proof of concept period or beta testing period as communicated by CyberArk or specified in an Order; (ii) the start date of any purchased version of such SaaS Products; or (iii) written notice of termination from CyberArk ("Trial Services Period"). CyberArk grants Customer, during the Trial Services Period, a non-exclusive, non- transferable right to access and use the Trial Services for Customer's internal evaluation purposes in accordance with the Documentation and subject to the access and use restrictions set forth in this Agreement. Customer is authorized to use Trial Services only for evaluation and not for any business or productive purposes, unless otherwise authorized by CyberArk in writing. Any data Customer enters into the Trial Services and any configurations made to the Trial Services by or for Customer during the term of such Trial Services will be permanently lost unless Customer: (a) has purchased a subscription to the same SaaS Products as covered by the Trial Services; or (b) exports such data or configurations before the end of such free period. There is no guarantee that features or functions of the Trial Services will be available, or if available will be the same, in the general release version of the SaaS Products, and Customer should review the SaaS Products features and functions before making a purchase. CyberArk will be under no obligation to provide Customer any support services with respect to the Trial Services. Notwithstanding anything to the contrary, CyberArk provides the Trial Services "as is" and "as available" without any warranties or representations of any kind. To the extent permitted by law, CyberArk disclaims all implied warranties and representations, including, without limitation, any implied warranty of merchantability, fitness for a particular purpose and non-infringement. Customer assumes all risks and all costs associated with its use of the Trial Services. Customer's sole and exclusive remedy in case of any dissatisfaction or CyberArk's breach of the Agreement with respect to such Trial Services is termination of the Trial Services. Any obligations on behalf of CyberArk to indemnify, defend, or hold harmless under this Agreement are not applicable to Customers using Trial Services.

1.5 **Third Party Materials.** The SaaS Products include Third-Party Materials, use of which is subject to their respective OSS Licenses as indicated in the Documentation. CyberArk warrants that the inclusion of such Third- Party Materials in the SaaS Products will not prevent Customer from exercising the license rights provided to Customer herein in respect of the SaaS Products or limit Customer's ability to use the SaaS Products in accordance with the Documentation. Nothing herein shall derogate from mandatory rights Customer may have under any OSS Licenses, if any. Customer may obtain a copy of the source code for certain Third-Party Materials by following the instructions set forth in the Documentation.

1.6 **Support.** As part of its provision of the SaaS Products, CyberArk shall make available technical support to Customer in accordance with the Support Services terms applicable to the SaaS Products. Upon notification from CyberArk, Customer shall promptly; update any Agents on Customer systems that interact with the SaaS Products; and/or as applicable ensure that all Authorized Users download and install all available updates for locally installed components without undue delay. Customer acknowledges and agrees that its failure to timely install such updates may result in disruptions to or failures of the SaaS Products, security risks or suspension of Customer's access to the SaaS Products, without any liability on the part of CyberArk to Customer.

1.7 **SaaS Product Usage Analytics.** CyberArk and its Affiliates shall be permitted to collect and use Usage Analytics for its reasonable business purposes and for Customer's benefit (including research and development statistical analyses, monitoring and management of CyberArk's Products). Other than for the purpose of providing the SaaS Products to Customer, in the event CyberArk discloses Usage Analytics or any part thereof to third parties (either during the Subscription Term of thereafter), such data shall be deidentified so that it will not identify Customer or its Authorized Users. The foregoing shall not limit in any way CyberArk's confidentiality obligations pursuant to Section 4 below.

2. Payment and Taxes

2.1. Payment Terms. Without prejudice to Customer's rights set out elsewhere in this Agreement, all SaaS Products fees are

non-refundable and payable in advance. CyberArk may invoice for purchases of SaaS Products upon delivery. Where:

(A) Customer is paying CyberArk directly, Customer shall pay all invoices within thirty (30) days of date of invoice, without any deduction or set-off (except for any amount disputed promptly and in writing by Customer in good faith), and payment will be sent to the address specified by CyberArk. Any amounts arising in relation to this Agreement not paid when due will be subject to a late charge of one and one-half percent (1 ½ %) per month on the unpaid balance or the maximum rate allowed by law, whichever is less; or

(B) Customer places an Indirect Order, CyberArk grants the rights described in this Agreement in consideration for and subject to: (a) Customer's agreement to comply with the pricing and payment terms of the Indirect Order, to be separately agreed between Customer and the applicable Channel Partner; and (b) Customer's agreement to comply with its obligations set forth in this Agreement (including the restrictions on use of the SaaS Products).

Notwithstanding the foregoing, the final sales price or rate shall be freely and independently determined between the applicable Channel Partner and Customer. For the avoidance of doubt, in the case of such an Indirect Order, any indication in this Agreement of an agreement between Customer and CyberArk for the price payable by Customer for such Indirect Order shall be null and void and not form a binding part of this Agreement and the provisions of this Agreement related to payment terms, pricing and/or order procedures shall not apply.

2.2 Taxes. The fees and charges covered by this Agreement are exclusive of any Indirect Taxes imposed or levied, currently or in the future based on applicable legislation, on the SaaS Products. Unless otherwise agreed between the Parties, Customer will be liable for compliance with reporting and payment of such Indirect Taxes in its tax jurisdiction. CyberArk shall include the Indirect Taxes on its invoice to Customer and remit such Indirect Taxes collected to the relevant authority if required by applicable law. CyberArk will be responsible for direct taxes imposed on CyberArk's net income or gross receipts in its tax jurisdiction. Notwithstanding the forgoing, all payments made under this Agreement shall be in cleared funds, without any deduction or set-off, and free and clear of and without deduction from any Indirect Taxes or other withholdings of any nature

3. Rights in Intellectual Property

3.1 **Intellectual Property.** Except for the rights granted in this Agreement, all rights, title, and interest in and to the SaaS Products. Documentation, and CyberArk Intellectual Property are hereby reserved by CyberArk, its Affiliates or licensors. Except as provided for herein, all rights, title, and interest in and to Customer Intellectual Property are hereby reserved by Customer, its Affiliates or licensors. Nothing in this Agreement shall transfer ownership of any Intellectual Property rights from one Party to the other.

3.2 **Customer Data.** Customer owns all right, title and interest in all Customer Data. Nothing in this Agreement shall be construed to grant CyberArk any rights in Customer Data beyond those expressly provided herein. Customer grants CyberArk and its Affiliates the limited, non-exclusive, worldwide license to view and use the Customer Data solely for the purpose of providing and improving the SaaS Products.

3.3 **Suggestions.** To the extent that Customer provides CyberArk with Suggestions, such Suggestions shall be free from any confidentiality restrictions that might otherwise be imposed upon CyberArk pursuant to this Agreement, and may be implemented by CyberArk in its sole discretion. Customer acknowledges that any CyberArk products or materials incorporating any such Suggestions shall be the sole and exclusive property of CyberArk.

3.4 **AI Features.** Certain features within the SaaS products use algorithmic analysis, artificial intelligence and/or machine learning technologies ("AI Features"). Use of the AI Features is subject to the Documentation and CyberArk's Responsible AI Policy found at https://www.cyberark.com/trust/responsible-ai/ Information regarding opting-out of AI Features is located in the Documentation.

4. Confidentiality

4.1 **Confidential Information.** The Parties acknowledge that each may disclose certain valuable confidential and proprietary information to the other Party. The receiving Party may only use the disclosing Party's Confidential Information to fulfill the purposes of this Agreement and in accordance with the terms of this Agreement. The receiving Party will protect the disclosing Party's Confidential Information by using at least the same degree of care as the receiving Party uses to protect its own Confidential Information of a

like nature (but no less than a reasonable degree of care) to prevent the unauthorized use, dissemination, disclosure or publication of such Confidential Information. Notwithstanding the foregoing, the receiving Party may disclose Confidential Information to its (and its Affiliates) employees, advisors, consultants, and agents on a need-to-know basis and provided that such party is bound by obligations of confidentiality substantially similar to those contained herein. This section 4 supersedes any and all prior or contemporaneous understandings and agreements, whether written or oral, between the Parties with respect to Confidential Information and is a complete and exclusive statement thereof. Additionally, the obligations set forth in section 5.4 and not this section 4 herein apply to Customer Data.

4.2 **Exceptions.** Information will not be deemed Confidential Information if it: (i) is known to the receiving Party prior to receipt from the disclosing Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; (ii) becomes known (independently of disclosure by the disclosing Party) to the receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; (iii) becomes publicly known or otherwise ceases to be secret or confidential, except through a breach of this Agreement by the receiving Party; (iv) is independently developed by the receiving Party without use of or reliance upon the disclosing Party's Confidential Information, and the receiving Party can provide evidence to that effect; or (v) is subject to the public records and meeting laws of the State of California, including the California Public Records Act (Government Code Section 6250 et seq.) and the California Brown Act (Government Code Section 54590 et seq.), and it is understood and agreed that Customer is a government entity and is required by law to disclose any of the above-described information, communications, and documents, Customer shall comply with such law and Customer has the right in its sole discretion to determine what shall be disclosed. Upon receiving notice of a Public Records Act (PRA) request from Customer, CyberArk shall notify Customer within 72 hours of any intent to challenge the disclosure legally. CyberArk acknowledges and understands that Customer is legally obligated to respond to the PRA requestor within 10 days. The receiving Party may disclose Confidential Information pursuant to the requirements of a court, governmental agency or by operation of law but shall (to the extent permissible by law) limit such disclosure to only the information requested and give the disclosing Party prior written notice sufficient to permit the disclosing Party to contest such disclosure.

4.3 **Advertising and Publicity.** Except as set forth in 4.2 above, Neither Party shall make or permit to be made any public announcement concerning the existence, subject matter or terms of this Agreement or relationship between the Parties without the prior written consent of the other Party. Notwithstanding the foregoing, it is expressly understood and agreed to by the parties that this Agreement may only be authorized by the Riverside County Board of Supervisors and shall be made publicly available for inspection for public meeting, which does not require advance written consent by CyberArk. Customer grants CyberArk and its Affiliates during the term of the Agreement the right to use Customer's trade names, logos, and symbols ("Customer Marks") in its public promotional materials and communications for the sole purpose of identifying Customer as a CyberArk customer. CyberArk shall not modify the Customer Marks, or display the Customer Marks any larger or more prominent on its promotional materials than the names, logos, or symbols of other CyberArk customers. The foregoing promotional materials and communications may be created, displayed, and reproduced without Customer's review, provided that they are in compliance with this section and any Customer Marks usage guidelines provided by Customer to CyberArk in writing.

5. Security and Processing of Personal Data

5.1 **Customer Data Content.** As between CyberArk and Customer, Customer is solely responsible for: (i) the content, quality and accuracy of Customer Data as made available by Customer and by Authorized Users; (ii) providing notice to Authorized Users with regards to how Customer Data will be collected and used for the purpose of the SaaS Products; (iii) ensuring Customer has a valid legal basis for processing Customer Data and for sharing Customer Data with CyberArk (to the extent applicable); and (iv) ensuring that the Customer Data as made available by Customer complies with applicable laws and regulations including Applicable Data Protection Laws.

5.2 **Data Protection Laws.** The Parties shall comply with their respective obligations under the Applicable Data Protection Laws. In particular, if Customer is established in the European Economic Area ("EEA"), in

Switzerland, in the United Kingdom ("UK") or in California, or will, in connection with the SaaS Products, provide CyberArk with personal data relating to an individual located within the EEA, Switzerland, the UK or California, the Parties shall comply with the Data Processing Addendum found at https://www.cyberark.com/CyberArk-Data-Processing- Addendum.pdf ("DPA") which in such case is hereby incorporated into this Agreement.

5.3 **HIPAA (Health Insurance Portability and Accountability Act)** Customer is a covered entity and includes "Protected Health Information" (as these terms are defined in the Business Associate Agreement ("BAA")) in Customer Data, the Parties shall comply with the terms of the BAA attached hereto and hereby incorporated into this Agreement by reference.

5.4 **Security of Customer Data.** CyberArk shall: (i) ensure that it has in place appropriate administrative, physical and technical measures designed to protect the security and confidentiality of Customer Data against any accidental or illicit destruction, alteration or unauthorized access or disclosure to third parties; and (ii) access and use the Customer Data solely to perform its obligations in accordance with the terms of this Agreement, and as otherwise expressly permitted in this Agreement. CyberArk shall not materially diminish its security controls with respect to Customer Data during a particular SaaS Products term. The obligations set forth in this Section 5.4 are in addition to any confidentiality, privacy, security or other requirements contained in the BAA or DPA, as applicable.

5.5 **Bring Your Own Key.** If Customer chooses to enable the "Bring Your Own Key" functionality for data encryption made available by CyberArk for certain SaaS Products ("BYOK"), Customer acknowledges that (i) Customer shall bear sole responsibility for the hosting, use, protection, rotation and management of such encryption key and any loss, damage, unavailability or non-performance resulting therefrom; (ii) Customer shall provide CyberArk with access to the encryption key at all times in order to encrypt Customer Data and proper performance of the SaaS Products; and (iii) CyberArk has no control over the encryption key and specifically is unable to de- encrypt, restore, recover or otherwise retrieve Customer Data in the event the encryption key is lost, damaged or otherwise not made available to CyberArk. If BYOK functionality is enabled by Customer, CyberArk disclaims any and all responsibility and liability for unavailability or non-performance of the SaaS Products caused by loss, damage or any unavailability of the encryption key.

6. Warranties

6.1 **Limited SaaS Products Warranty.** During the applicable Subscription Term, CyberArk warrants that: (a) the SaaS Products will perform in substantial conformity with the Documentation; and (b) CyberArk will use industry standard measures designed to detect viruses, worms, Trojan horses or other unintended malicious or destructive code in the SaaS Products. The foregoing warranties are void if the failure of the SaaS Products has resulted from negligence, error, or misuse of the SaaS Products (including use not in accordance with the Documentation) by Customer, the Authorized User or by anyone other than CyberArk. Customer shall be required to report any breach of warranty to CyberArk within a period of thirty (30) days of the date on which the incident giving rise to the claim occurred. CyberArk's sole and exclusive liability, and Customer's sole and exclusive remedy, for breach of these warranties will be for CyberArk, at its expense, to use reasonable commercial efforts to correct such nonconformity within thirty (30) days of the date that notice of the breach was provided; and, if CyberArk fails to correct the breach within such cure period, Customer may terminate the affected Order and, in such event, CyberArk shall provide Customer with a pro-rata refund of any unused pre-paid fees paid for the period following termination as calculated on a monthly basis for the affected SaaS Products. Without derogating from CyberArk's obligations under this Agreement, Customer warrants that it shall take and maintain appropriate steps within its control to protect the confidentiality, integrity, and security of its Confidential Information and Customer Data, including: (i) operating the SaaS Products in accordance with the Documentation and applicable law and; and (ii) dedicating reasonably adequate personnel and resources to implement and maintain the security controls set forth in the Documentation. Customer will be responsible for the acts and omissions of its Authorized Users.

6.2 **Compliance with Law.** Each Party shall comply with all applicable, laws and regulations in connection with the performance of its obligations and the exercise of its rights under this Agreement.

6.3 **Disclaimer.** Any and all warranties, expressed, incorporated or implied, are limited to the extent and period mentioned in this Agreement. To the maximum extent allowed by applicable law, CyberArk disclaims (and disclaims on behalf of its licensors and/or contributors to any Third-Party Materials) all other warranties, conditions and other terms, whether express or implied or incorporated into this Agreement by statute, common law or otherwise, including the implied conditions and warranties of merchantability and fitness for a particular purpose. CyberArk will have no responsibility or liability for delays, failures or losses (i) attributable or related in any way to the use or implementation of third-party hardware, software or services not provided by CyberArk; or (ii) use of the SaaS Products not in accordance with the Documentation.

7. Indemnification

7.1 **Infringement Indemnity.** CyberArk shall defend and indemnify Customer and/or its Affiliates and their officers, directors and employees against all third-party claims, suits and proceedings and all directly related losses, liabilities, damages, costs and expenses (including reasonable attorneys' fees) resulting from the violation, misappropriation, or infringement of such third party's patent, copyright, trademark or trade secret caused by Customer's use of the SaaS Products in accordance with this Agreement and the Documentation.

7.2 **Hold Harmless.** CYBERARK shall indemnify and hold harmless Customer, its Departments, and/or its Affiliates and their employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) acting on its behalf, from any third party liability, action, claim or damage whatsoever, directly arising out of property damage, bodily injury, or death caused by CyberArk, its officers, employees, subcontractors, or personnel. CYBERARK shall defend the Indemnitees at its sole expense including all direct costs and fees (including, but not limited, to attorney fees, cost of investigation, defense and settlements or awards) in any third party claim or action based upon such, death, bodily injury, or damage to real or tangible property. CYBERARK'S obligation hereunder shall be satisfied when CYBERARK has provided to Customer the appropriate form of dismissal relieving Customer from any liability for the third party action or claim involved. The specified insurance limits required in this Agreement shall in no way limit or circumscribe CYBERARK'S obligations to indemnify and hold harmless the Indemnitees herein from third party claims.

7.3 **Customer Data and Use Indemnity.** Customer shall defend and indemnify CyberArk and/or its Affiliates and their officers, directors and employees against any third-party claims, suits and proceedings (including those brought by a government entity), and all directly related losses, liabilities, damages, costs and expenses (including reasonable attorneys' fees) resulting from: (i) an alleged infringement or violation by the Customer Data of such third-party's patent, copyright, trademark, trade secret; or (ii) CyberArk's use of the Customer Data violating applicable law, provided that such use is in accordance with the terms of this Agreement and (where applicable) with the terms of the DPA and/ or the BAA.

7.4 **Process.** Each Party's defense and indemnification obligations herein will become effective upon, and are subject to: (a) the indemnified Party's prompt notification to the indemnifying Party of any claims in writing; and (b) the indemnified Party providing the indemnifying Party with full and complete control, authority and information for the defense of the claim, provided that the indemnifying Party will have no authority to enter into any settlement or admission of the indemnified Party's wrongdoing on behalf of the indemnified Party without the indemnified Party's prior written consent (not to be unreasonably withheld). At the indemnifying Party's request, the indemnified Party shall reasonably cooperate with the indemnifying Party in defending or settling any claim.

7.5 **Exclusions.** The above CyberArk obligations to defend and indemnify will not apply in the event that a claim arises from or relates to: (a) use of the SaaS Products not in accordance with the Documentation and this Agreement; (b) Customer's use of the SaaS Products in violation of applicable laws; (c) any modification, alteration or conversion of the SaaS Products not created or approved in writing by CyberArk; (d) any combination or use of the SaaS Products with any computer, hardware, software, data or service not provided by CyberArk if the claim would not have arisen but for such combination or use; (e) CyberArk's compliance with specifications, requirements or requests of Customer ; or (f) Customer's gross negligence or willful misconduct.

7.6 **Remedies.** If a SaaS Product becomes, or CyberArk reasonably determines that a SaaS Product is likely to become, subject to a claim of infringement for which CyberArk must indemnify Customer as described above, CyberArk may at its option and expense: (a) procure for Customer the right to continue to access and use that SaaS Product, (b) replace or modify that SaaS Product so that it becomes non-infringing without causing a material adverse effect on the functionality provided by that SaaS Product, or (c) if neither of the foregoing options are available in a timely manner on commercially reasonable terms, terminate the affected Order and provide Customer with a pro-rata refund of any unused pre-paid fees paid for the period following termination as calculated on a monthly basis for that SaaS Product. This section titled "Indemnification" states the sole liability of CyberArk and the exclusive remedy of Customer with respect to any indemnification claims arising out of or related to this Agreement.

8. Limitation of Liability

8.1 **Maximum Liability.** Except for liability caused by CyberArk's intellectual property infringement indemnification obligations in section 7.1, section 7.2, Customer's data infringement indemnity in section 7.3, Customer's payment obligations herein, or a party's breach of the BAA (which will be subject to the Super Cap), in no event will either Party's maximum aggregate liability arising out of or related to this Agreement, regardless of the cause of action and whether in contract, tort, (including negligence) warranty, indemnity or any other legal theory, exceed five (5) times the total amount paid or payable to CyberArk under this Agreement during the twelve (12) month period preceding the date of initial claim ("Base Cap"). Solely with respect to liability caused by a party's breach of the BAA, the Base Cap will apply, but will be increased to an amount equal to the greater of: seven (7) times the total amount paid or payable to CyberArk under this Agreement during the twelve (12) month period preceding the date of the initial claim, or $2,500,000 ("Super Cap").

8.2 **No Consequential Damages.** Neither Party will have any liability to the other Party for any loss of profits or revenues, loss of goodwill, or for any indirect, special, incidental, consequential or punitive damages arising out of, or in connection with this Agreement, however caused, whether in contract, tort (including negligence), warranty, indemnity or any other legal theory, and whether or not the Party has been advised of the possibility of such damages.

8.3 **Construction.** This Agreement is not intended to and will not be construed as excluding or limiting any liability which cannot be limited or excluded by applicable law, including liability for (a) death or bodily injury caused by a Party's negligence; or (b) gross negligence, willful misconduct, or fraud.

9. **Assignment.** Neither Party may assign any of its rights or obligations under this Agreement without the other Party's prior written consent, which will not be unreasonably withheld. Notwithstanding the foregoing, either Party may assign any and all of its rights and obligations under this Agreement to a successor in interest in the event of a merger or acquisition or to an Affiliate, upon written notice to the other Party.

10. **Restricted Rights and Export Control**

10.1 **Export Control.** The exportation of the SaaS Products and Documentation, and all related technology and information thereof are subject to U.S. laws and regulations pertaining to export controls and trade and economic sanctions, including the U.S. Export Administration Act, Export Administration Regulations, the Export Control Reform Act, and the Office of Foreign Assets Control's sanctions programs, the laws of the State of Israel, and the laws of any country or organization of nations within whose jurisdiction Customer (or its Authorized Users who may use or otherwise receive the SaaS Products as expressly authorized by this Agreement) operates or does business, as amended, and the rules and regulations promulgated from time to time thereunder. Specifically, Customer hereby undertakes not to export, re-export, access or grant access to the SaaS Products and all related technology, information, materials and any upgrades thereto to: (a) any Prohibited Persons; (b) any country to which such export, re-export or access from is restricted or prohibited per the foregoing applicable laws; or (c) otherwise in violation of any applicable export or import restrictions, laws or regulations. Customer also certifies that it is not a Prohibited Person nor owned, controlled by, or acting on behalf of a Prohibited Person.

10.2 **Commercial Computer Software and FedRAMP Products.** If Customer is an agency or contractor of the United States Government, Customer acknowledges and agrees that: (i) the SaaS Products (including any software forming a part thereof) were developed entirely at private expense; (ii) the SaaS Products (including any software forming a part thereof) in all respects constitute proprietary data belonging solely to CyberArk; (iii) the SaaS Products (including any software forming a part thereof) are not in the public domain; and (iv) the software forming a part of the SaaS Products is "Commercial Computer Software" as defined in sub-paragraph (a)(1) of DFARS section 252.227-7014 or FAR Part 12.212. Customer shall provide no rights in the Software (including any software forming a part thereof) to any U.S. Government agency or any other party except as expressly provided in this Agreement. If Customer places an Order for SaaS Products which are designated as "FedRAMP Authorized," the CyberArk Rider to SaaS Terms of Service for FedRAMP Products found at https://www.cyberark.com/contract- terms/ is incorporated herein and will apply to CyberArk's provision of such SaaS Products.

11. **Professional Services.** Customer may separately purchase from CyberArk professional services in relation to the SaaS Products as may be generally available by CyberArk to its customers, pursuant to CyberArk's then applicable professional services terms.

12. **Term and Termination.**

12.1 **Term**. This Agreement will be effective upon the Effective Date and shall remain in force for 1 year unless or until terminated by either Party pursuant to this section; provided, however, to the extent that any Orders remain active past the Term of this Agreement, such Orders will continue to be governed by this Agreement until the expiration or termination thereof.

12.2 **Termination.** Either Party may terminate this Agreement immediately upon notice to the other Party if the other Party: (i) materially breaches this Agreement and fails to remedy such breach within thirty (30) days after receiving written notice of the breach from the other Party; (ii) commences bankruptcy or dissolution proceedings, has a receiver appointed for a substantial part of its assets or ceases to operate in the ordinary course of business. In addition, a Party may terminate this Agreement, a SOW, or an Order, in whole or in part, or cease provision of the SaaS Products if required to comply with applicable law or regulation, and such termination will not constitute a breach of this Agreement by the terminating Party. CyberArk reserves the right to suspend Customer's access to the applicable SaaS Products upon written notice to Customer if: (a) an invoice is more than thirty (30) days past due; or (b) a material breach of this Agreement fails to be cured within thirty (30) days. CyberArk will promptly reinstate Customer's access and use of the SaaS Products/provision of the Professional Services once the issue has been resolved. Upon termination or expiration of the Agreement or an Order, (x) any accrued rights and obligations will survive; (y) all outstanding fees and other charges under the Agreement or Order (as applicable) will become immediately due and payable, and (z) Customer will have no further right to access or use the applicable SaaS Products or professional services. If Customer is converting its perpetual self-hosted software licenses to a SaaS Product, the applicable previously licensed perpetual self-hosted software licenses will be terminated, along with any associated support services, in accordance with the terms of the applicable Order.

12.3 **Effects of Termination/Expiration.** Upon termination or expiration of an applicable Subscription Term, CyberArk may immediately deactivate Customer's account, and: (i) Customer will have no further right to access or use the SaaS Products, except for the limited right to access or use the SaaS Products for purposes of exporting Customer Data in accordance with the applicable Documentation; and (ii) each Party shall return or destroy any tangible Confidential Information of the other Party within its possession or control that is not contained on the SaaS Products promptly upon receiving written request from the other Party. Customer acknowledges that it is responsible for exporting any Customer Data to which Customer desires continued access after termination/expiration, and CyberArk shall have no liability for any failure of Customer to retrieve such Customer Data and no obligation to store or retain any such Customer Data beyond 40 days following termination or expiration of the Customer's Subscription Term. Any Customer Data contained on the SaaS Products will be deleted within 60 days of termination or expiration of Customer's Subscription Term.

12.4 **Non-appropriations.** In the event funds are not appropriated by the applicable federal, state, and/or local agency during any fiscal period of the subscription term set forth in the applicable quote, the Order(s) may be terminated by Customer upon written notification to CyberArk, to include a copy of the non-appropriation of funds notification, as of the beginning of the fiscal year for which funds are not appropriated or otherwise secured, provided that Customer (a) agrees to include in its budget request appropriations sufficient to cover Customer's obligations under the Order; and (b) agrees it will not use non-appropriations as a means of terminating the Order(s) in order to acquire functionally equivalent products or services from a third party. In the event Customer terminates the Order(s) under this provision, neither party shall have any further obligation to the other party with respect to such Order, excepting Customer shall be responsible for the payment of any and all unpaid charges for products and services rendered under such Order(s) prior to the non-appropriated fiscal period, all of which are to be paid by Customer to CyberArk within thirty (30) days of the invoice date. Customer shall notify CyberArk in writing as soon as it has knowledge that funds are not available for any fiscal period under the applicable Order's Subscription Term.

13. Miscellaneous

13.1 **Independent Contractors.** Nothing in this Agreement will be construed to imply a joint venture, partnership or principal-agent relationship between CyberArk and Customer, and neither Party will have the right, power or authority to obligate or bind the other in any manner whatsoever.

13.2 **Notices.** All Notices will be in writing and will be deemed to have been duly given: (a) when delivered by hand; (b) three (3) days after being sent by registered or certified mail, return receipt requested and postage prepaid; (c) one (1) day after deposit with a nationally recognized overnight delivery or express courier service; or (d) when provided via email when the sender has received a delivery/read receipt. Notices for CyberArk should be sent to the following addresses: (i) for physical Notices the address specified for CyberArk in section 13.4 "Governing Law and Jurisdiction" and; (ii) for electronic Notices to: contract-notices@cyberark.com. In the event that Customer has any technical support-related queries, the contact information for support can be found at: https://www.cyberark.com/customer-support/.

13.3 **Force Majeure.** With the exception of Customer's payment obligations herein, neither Party will be liable to the other Party for any delay or failure to perform which is due to fire, local outbreak, epidemic, and pandemic travel advisories as to health, security and/or terrorism, flood, lockout, transportation delay, war, acts of God, governmental rule or order, strikes or other labor difficulties, or other causes beyond its reasonable control. However, local outbreak, epidemic, and pandemics shall only apply if they are accompanied by governmental orders, directives, or regulations that materially impede, delay, or prevent the performance of the affected party's obligations under this agreement and in such event, both Parties will resume performance promptly after the cause of such delay or failure has been removed.

13.4 **Governing Law and Jurisdiction.** Each Party agrees to the applicable governing law below without regard to choice or conflicts of law rules, and to the exclusive jurisdiction of the applicable courts below with respect to any dispute, claim, action, suit or proceeding (including non-contractual disputes or claims) arising out of or in connection with this Agreement, or its subject matter or formation. To the extent not prohibited by applicable law, each of the Parties hereby irrevocably waives any and all right to trial by jury in any legal proceeding arising out of or related to this Agreement.

CyberArk entity entering into Agreement:	With Principal Office at:	Choice of Law:	Exclusive Jurisdiction:
CyberArk Software, Inc.	60 Wells Avenue, Newton, MA 02459, U.S.A.	Laws of the state of California, U.S.A.	Courts of Riverside County, California, U.S.A.

13.5 **Disputes**. The Parties shall attempt to resolve any disputes, claims, or controversies arising out of or relating to this Agreement through good faith negotiations at the working level, including escalation to the senior management of the Parties as needed. Both Parties shall proceed diligently with the performance of this Agreement pending the resolution of a dispute. If the dispute cannot be resolved through negotiations within thirty (30) days, it shall be resolved by binding arbitration administered by a renowned institution such as the American Arbitration Association (AAA), the London Court of International Arbitration (LCIA), or the International Chamber of Commerce (ICC), in accordance with their respective rules, The arbitration shall be conducted in English. The location of the arbitration shall be as set forth in Section 13.4. The arbitration process shall be conducted expeditiously, with clear timelines established to avoid undue delay. The arbitration process shall be conducted expeditiously, with clear timelines established to avoid undue delay. The arbitrator shall be instructed to render a final decision within six (6) months from the date of appointment. The arbitration shall be conducted by a single arbitrator, selected by mutual agreement of the parties. If the parties cannot agree on an arbitrator, the administering institution shall appoint one. Arbitration shall be the exclusive means of resolving any disputes arising out of or relating to this Agreement. The parties waive their right to seek remedies in court, except for the enforcement of the arbitration award. The parties agree that any arbitration shall be conducted on an individual basis only, and not as a class action or other representative action. The arbitrator shall have no authority to conduct any class, collective, or representative proceeding. The parties agree that the arbitration shall be confidential, and neither party shall disclose the existence, content, or results of the arbitration, except as may be required by law or for purposes of enforcement of the arbitration award.

13.6 **Entire Agreement, Execution, and Modification.** This Agreement supersedes all prior agreements and representations between the Parties regarding the subject matter of this Agreement. The terms and conditions contained in any Order issued by Customer will be of no force or effect, even if the Order is accepted by CyberArk. CyberArk may request changes to these Terms of Service from time to time. If CyberArk requests a material change to any of the foregoing, the parties may agree by written amendment. This Agreement may be executed in counterparts, each of which when executed and delivered shall constitute a duplicate original, but shall together constitute one agreement. Transmission of an executed counterpart of this Agreement or the executed signature page of a counterpart of this Agreement by: (a) email (in PDF, JPEG or other agreed format); or (b) a generally recognized electronic signature program, shall take effect as delivery of an executed counterpart of this Agreement. No counterpart shall be effective until each Party has executed and delivered at least one counterpart. This Agreement may not be amended other than by a written instrument specifically intended for this sole purpose and signed by the authorized representatives of both Parties.

13.7 **Severability and Waiver.** This Agreement shall be deemed severable, and the invalidity or unenforceability of any term or provision hereof shall not affect the validity or enforceability of this Agreement or of any other term or provision hereof. Should any term or provision of this Agreement be declared void or unenforceable by any court of competent jurisdiction, the Parties intend that a substitute provision will be added to this Agreement that, to the greatest extent possible, achieves the intended commercial result of the original provision. The failure of either Party to enforce any rights granted to it hereunder or to take action against the other Party in the event of any breach hereunder will not be deemed a waiver by that Party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

13.8 **No Exclusions.** Each Party hereby represents and warrants to the other that (a) it is not excluded from any federal health care program, as defined under 42 U.S.C. Section 1320a-7b(f), for the provision of items or services for which payment may be made under a federal health care program; (b) no basis for exclusion from any health care program exists; (c) it has not arranged or contracted (by employment or otherwise) with any employee, contractor, or agent that the party knows or should know are excluded from participation in any federal health care program; and (d) no final adverse action, as such term is defined under 42 U.S.C. Section 1320a-

7e(g), has occurred or is pending or threatened against the party (collectively, "Exclusions/Adverse Actions"). Each Party shall notify the other of any Exclusions/Adverse Actions or any basis therefor within fifteen (15) days of its learning of any such Exclusions/Adverse Actions or any basis therefor.

13.9 **INSURANCE**. During the applicable license term/Subscription Term, CyberArk shall carry and maintain, at its own expense, the following types and amounts of insurance with insurers having an A.M. Best rating of A- or better:

(a) Workers' Compensation insurance with benefits afforded under the laws of the state in which the Services are to be performed or alternative plan or coverage as permitted or requested by the applicable law in the jurisdiction where work is performed; including Employers Liability insurance with limits of $1,000,000 for each accident or disease and in the aggregate;
(b) Commercial General Liability insurance with limits of $1,000,000 and $2,000,000 in the aggregate covering liability arising from premises, operations, personal injury, and products/completed operations.
(c) Umbrella liability policy with limits of liability of $5,000,000 per claim and in the aggregate.
(d) A combined **Technology Professional Liability Errors and Omissions Insurance and Cyber Liability Insurance**, appropriate to CyberArk's profession and work hereunder, with limits not less than $2,000,000 per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CyberArk in this Agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy does not cover patent and trade secret infringements. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses. The Policy shall include coverage for damage to, alteration of, loss of, or destruction of electronic data. All certificates of insurance may name "Customer, its subsidiaries and affiliates" as an additional insured with respect to General Liability coverages only. Should any of the above described policies be cancelled before the expiration date thereof, notice will be delivered in accordance with the policy provisions.

13.10 **Definitions and Interpretation.** The following definitions and rules of interpretation apply in this Agreement:

"Affiliate" means a company controlling, controlled by, or under common control with a Party (an entity will be deemed to have control if it owns over 50% of another entity or the ability to direct the management of the entity by contract or otherwise).

"Agents" means CyberArk's proprietary software, systems and locally-installed software agents and connectors including mobile applications that interact with the SaaS Products as may be provided by CyberArk in connection with the SaaS Products.

"Applicable Data Protection Laws" means all applicable privacy and data protection laws, their implementing regulations, regulatory guidance and secondary legislations, each as updated or replaced from time to time, including: (a) the General Data Protection Regulation (EU 2016/679) (the "GDPR") and any applicable national implementing laws; (b) the UK General Data Protection Regulation ("UK GDPR") and the UK Data Protection Act 2018; (c) the Privacy and Electronic Communications Directive (2002/ 58/ EC) and any applicable implementing laws, including the Privacy and Electronic Communications

Regulations 2003 (SI 2003/ 2426) ("EC Directive"); (d) the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); (e) U.S. legislation (e.g. the California Consumer Privacy Act ("CCPA") and the California Privacy Rights Act ("CPRA"); and (f) any other laws that may be applicable.

"Authorized Users" means employees, agents, consultants, contractors, or vendors authorized by Customer to use the SaaS Products solely for the internal use of Customer and its Affiliates, subject to the terms and conditions of this Agreement. For the avoidance of doubt, licenses associated with SaaS Products purchased as a bundle (under a single product code) cannot be separated between different Authorized Users.

"Channel Partner" means a third-party business entity that CyberArk has appointed as an approved partner to as applicable, distribute, re-sell and support the SaaS Products.

"Confidential Information" means all information provided by the disclosing Party to the receiving Party concerning the disclosing Party or its Affiliates' business, products or services that is not generally known to the public, including information relating to customers, vendors, trade secrets, prices, products, services, computer programs and other intellectual property and any other information which a Party should reasonably understand to be considered Confidential Information whether or not such information is marked "Confidential" or contains such similar legend by the disclosing Party at the time of disclosure.

"Customer Data" means all data and/or content uploaded to the SaaS Products by Customer (including where applicable Authorized Users), and in all data derived from it (other than Usage Analytics).

"CyberArk" means the CyberArk legal entity providing the SaaS Product to Customer pursuant to this Agreement, at the address specified in section 13.4 "Governing Law and Jurisdiction.

"Documentation" means the user guides, installation documents, and specifications for the SaaS Products that are made available from time to time by CyberArk in electronic or tangible form and found at docs.cyberark.com, including the documentation located therein under the 'Security' section for the relevant SaaS Products, but excluding any sales or marketing materials.

"Indirect Order" means an Order for the Software or Services from a Channel Partner of Customer's choosing pursuant to an independent commercial agreement.

"Indirect Taxes" means excise, sales, use, gross-turnover, value added, goods and services tax or other similar types of indirect taxes on turnover and/or revenues, duties, customs or tariffs (however designated, levied or based and whether foreign or domestic, federal, state or province).

"Intellectual Property" means a Party's proprietary material, technology, or processes (excluding the SaaS Products and Documentation), including services, software tools, proprietary framework and methodology, hardware designs, algorithms, objects and documentation (both printed and electronic), network designs, know- how, trade secrets and any related intellectual property rights throughout the world (whether owned or licensed by a third party) and any derivatives, improvements, enhancements or extensions of such Intellectual Property conceived, reduced to practice, or developed.

"Notice" means any formal legal notice or equivalent communication required or permitted under this Agreement.

"Order" means CyberArk's quote accepted by Customer via Customer's purchase order or other ordering document received by CyberArk (directly or indirectly through a Channel Partner) to order CyberArk's SaaS Products, which references the SaaS Products, pricing, payment terms, quantities, expiration date and other applicable terms set forth in an applicable CyberArk quote or ordering document.

"OSS Licenses" means the respective open source licenses that the Third-Party Materials are subject to.

"Prohibited Persons" means anyone on the U.S. Commerce Department's Denied Persons, Entity, or Unverified Lists or the U.S. Treasury Department's list of Specially Designated Nationals and Consolidated Sanctions list.

"SaaS Products" means the software-as-a-service products specified in the Order as further described in the Documentation (including any updates and upgrades to the SaaS Products provided by CyberArk in its sole discretion, and any software, systems and locally-installed software agents and connectors that interact with the SaaS Products as may be provided by CyberArk in connection with the SaaS Products), provided that any free trial SaaS software, proof of concept of the SaaS Products, beta version of the SaaS Products, or any other free-of- charge software product will be subject to Section 1.4 of this Agreement.

"Subscription Term" means the period of time during which Customer is subscribed to the SaaS Products, as specified in an Order and which shall begin upon delivery of the SaaS Products.
"Suggestions" means, any feedback, ideas or suggestions for improvements, new features, customer experience, functionalities, corrections, enhancements or changes to the SaaS Products suggested by Customer to CyberArk, excluding any Customer Data and Customer Intellectual Property.

"Support Services" means the maintenance and technical support services for the SaaS Products provided by CyberArk to Customer as part of an active SaaS Products subscription, set out at https://www.cyberark.com/maintenance-support-terms.pdf.

"Third-Party Materials" means open source software programs that are made available by third parties under their respective OSS Licenses.

"Usage Analytics" means data generated or collected in connection with Customer's access, use and configuration of the SaaS Products and data derived from it (e.g. metadata, types of applications or accounts utilized or interacting with the SaaS Products).

Any words following the terms including or include shall be regarded as examples only and not construed as an exhaustive list.

[Intentionally Left Blank; Signature Page Follows]

IN WITNESS WHEREOF, the Parties have executed this Agreement by their duly authorized representatives.

CyberArk Software, Inc.:

Signature Signed by: Jenny Hayes 343A8F3459E14C5... **Name** Jenny Hayes **Title** VP Revenue **Date** April 17, 2025

Customer: County of Riverside, on behalf of Riverside University Health System

Signature V. M. P. **Name** V. MANUEL PEREZ **Title** CHAIR, BOARD OF SUPERVISORS **Date** JUN 10 2025

ATTEST:

Kimberly A. Rector

Clerk of the Board

By: _____

Title: DEPUTY

APPROVED AS TO FORM:

Minh C. Tran

County Counsel

By: Esen Sainz

Esen Sainz

Deputy County Counsel

Date: 06/03/2025

JUN 10 2025 18.3

HIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and CyberArk Software, Inc.

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of the SaaS Terms of Service, or other written agreement governing Contractor's provision of software-as-a-service products ("SaaS Products") to County (the "Underlying Agreement") between the County of Riverside ("County") and CyberArk Software, Inc., a Delaware corporation ("Contractor") and shall be effective as of the date the Underlying Agreement is approved by both Parties (the "Effective Date").

RECITALS

WHEREAS, County and Contractor entered into the Underlying Agreement pursuant to which the Contractor provides services to County, and in conjunction with the provision of such services certain protected health information ("PHI") and/or certain electronic protected health information ("ePHI") may be provided to or made available to Contractor for the purposes of carrying out its obligations under the Underlying Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191 enacted August 21, 1996, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 enacted February 17, 2009, and the laws and regulations promulgated subsequent thereto, as may be amended from time to time, are applicable to the protection of any use or disclosure of PHI and/or ePHI pursuant to the Underlying Agreement; and,

WHEREAS, County is a covered entity, as defined in the Privacy Rule; and,

WHEREAS, to the extent County discloses PHI and/or ePHI to Contractor or County or County users create, receive, maintain, or transmit PHI and/or ePHI of County as part of the services under the Underlying Agreement such that Contractor is deemed to be acting as County's business associate, as defined in the Privacy Rule; and,

WHEREAS, pursuant to 42 USC §17931 and §17934, certain provisions of the Security Rule and Privacy Rule apply to a business associate of a covered entity in the same manner that they apply to the covered entity, the additional security and privacy requirements of HITECH are applicable to business associates and must be incorporated into the business associate agreement, and a business associate is liable for civil and criminal penalties for failure to comply with these security and/or privacy provisions; and,

WHEREAS, the parties mutually agree that any use or disclosure of PHI and/or ePHI must be in compliance with the Privacy Rule, Security Rule, HIPAA, HITECH and any other applicable law; and,

WHEREAS, the parties intend to enter into this Addendum to address the requirements and obligations set forth in the Privacy Rule, Security Rule, HITECH and HIPAA as they apply to Contractor as a business associate of County, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by Contractor during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HITECH, HIPAA, Security Rule and/or Privacy Rule, as may be amended from time to time.

   A. "Breach" when used in connection with PHI means the acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of the Privacy Rule which compromises the security or privacy of the PHI, and shall have the meaning given such term in 45 CFR §164.402.

      (1) Except as provided below in Paragraph (2) of this definition, acquisition, access, use, or disclosure of PHI in a manner not permitted by subpart E of the Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

         (a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

         (b) The unauthorized person who used the PHI or to whom the disclosure was made;

         (c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated.

(2) Breach excludes:

(a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the Privacy Rule.

(b) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by subpart E of the Privacy Rule.

(c) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. "Business associate" has the meaning given such term in 45 CFR §164.501, including but not limited to a subcontractor that creates, receives, maintains, transmits or accesses PHI on behalf of the business associate.

C. "Data aggregation" has the meaning given such term in 45 CFR §164.501.

D. "Designated record set" as defined in 45 CFR §164.501 means a group of records maintained by or for a covered entity that may include: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or, used, in whole or in part, by or for the covered entity to make decisions about individuals.

E. "Electronic protected health information" ("ePHI") as defined in 45 CFR §160.103 means protected health information transmitted by or maintained in electronic media, limited to the information created or received by Contractor from or on behalf of County.

F. "Electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given such term in 42 USC §17921(5).

G. "Health care operations" has the meaning given such term in 45 CFR §164.501.

H. "Individual" as defined in 45 CFR §160.103 means the person who is the subject of protected health information.

I. "Person" as defined in 45 CFR §160.103 means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

J. "Privacy Rule" means the HIPAA regulations codified at 45 CFR Parts 160 and 164, Subparts A and E.

K. "Protected health information" ("PHI") has the meaning given such term in 45 CFR §160.103, which includes ePHI, limited to the information created or received by Contractor from or on behalf of County.

L. "Required by law" has the meaning given such term in 45 CFR §164.103.

M. "Secretary" means the Secretary of the U.S. Department of Health and Human Services ("HHS").

N. "Security incident" as defined in 45 CFR §164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

O. "Security Rule" means the HIPAA Regulations codified at 45 CFR Parts 160 and 164, Subparts A and C.

P. "Subcontractor" as defined in 45 CFR §160.103 means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Q. "Unsecured protected health information" and "unsecured PHI" as defined in 45 CFR §164.402 means PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of a technology or methodology specified by the Secretary in the guidance issued under 42 USC §17932(h)(2), and limited to the information created or received by Contractor from or on behalf of County.

2. **Scope of Use and Disclosure by Contractor of County's PHI and/or ePHI.**

A. The parties hereby agree that this Addendum does not apply: (1) to any other Contractor product, service, or feature not part of the services contemplated under the Underlying Agreement; (2) to any data other than pHI that may be disclosed to Contractor (including unintentionally or mistakenly) pursuant to the Underlying Agreement,; or (3) in any other manner from a geography other than the United States. Except as otherwise provided in this Addendum, Contractor may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Contractor under the Underlying Agreement or to perform functions, activities or services for, or on behalf of, County as specified in this Addendum, if such use or disclosure does not violate HIPAA, HITECH, the Privacy Rule and/or Security Rule.

B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Addendum or required by law, in accordance with 45 CFR §164.504(e)(2), Contractor may:

1) Use PHI and/or ePHI if necessary for Contractor's proper management and administration and to carry out its legal responsibilities, including to enable judicial or administrative proceedings and law enforcement purposes; and,

2) Disclose PHI and/or ePHI for the purpose of Contractor's proper management and administration or to carry out its legal responsibilities, including to enable judicial or administrative proceedings and law enforcement purposes, only if:

a) The disclosure is required by law; or,

b) Contractor obtains reasonable assurances, in writing, from the person to whom Contractor will disclose such PHI and/or ePHI that the person will:

i. Hold such PHI and/or ePHI in confidence and use or further disclose it only for the purpose for which Contractor disclosed it to the person, or as required by law; and,

ii. Notify Contractor of any instances of which it becomes aware in which the confidentiality of the information has been breached; and,

3) Use PHI to provide data aggregation services relating to the health care operations of County pursuant to the Underlying Agreement or as requested by County; and,

4) De-identify all PHI and/or ePHI of County received by Contractor under this Addendum provided that the de-identification conforms to the requirements of the Privacy Rule and/or Security Rule and does not preclude timely payment and/or claims processing and receipt.

C. Notwithstanding the foregoing, in any instance where applicable state and/or federal laws and/or regulations are more stringent in their requirements than the provisions of HIPAA, including, but not limited to, prohibiting disclosure of mental health and/or substance abuse records, the applicable state and/or federal laws and/or regulations shall control the disclosure of records.

3. **Prohibited Uses and Disclosures.**

A. Contractor may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without patient authorization or de-identification of the PHI and/or ePHI and as authorized in writing from County.

B. Contractor may neither use, disclose, nor access PHI and/or ePHI it receives from County or from another business associate of County, except as permitted or required by this Addendum, or as required by law.

C. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.

D. Contractor shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Contractor agrees:

1) Not to use or disclose PHI for fundraising , unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;

2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);

3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,

4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by County to Contractor for services provided pursuant to the Underlying Agreement.

4. **Obligations of County.**

A. County agrees to make its best efforts to notify Contractor promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by County that may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.

B. County agrees to make its best efforts to promptly notify Contractor in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.

C. County agrees to make its best efforts to promptly notify Contractor in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect Contractor's use or disclosure of PHI and/or ePHI. County has included, and will include, in its notice of privacy practices a statement that County may disclose PHI for treatment, payment, healthcare operations purposes, and any other purpose which relates to the services provided by Contractor to County.

D. County agrees not to request Contractor to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule or that would not be permissible under such HITECH, HIPAA, the Privacy Rule and/or Security Rule if so used or disclosed by County (except for the purposes specified under 45 CFR § 164.504(e)(2)(i)(A) and (B)).

E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

F. Where the compliance with a requirement of this Addendum requires actual knowledge by Contractor as to whether PHI or ePHI is involved, County shall advise Contractor regarding PHI or ePHI content, and any other details regarding such PHI or ePHI as necessary for Contractor's performance of this Addendum.

G. County represents and warrants that it will disable or not use any functionality on Contractor's SaaS Products other than the services contemplated under the Underlying Agreement that would otherwise disclose PHI or ePHI to Contractor, and will instruct its users to do the same.

5. **Obligations of Contractor.** In connection with the use or disclosure of PHI and/or ePHI, Contractor agrees to:

A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of 45 CFR §164.504(e). Contractor shall also comply with the additional privacy requirements that are applicable to covered entities in HITECH, as may be amended from time to time.

B. Not use or further disclose PHI and/or ePHI other than as permitted or required by this Addendum or as required by law. Contractor shall, to the extent permitted by law, promptly notify County if Contractor is required by law to disclose PHI and/or ePHI.

C. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Addendum.

D. Mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI and/or ePHI by Contractor in violation of this Addendum.

E. Report to County any use or disclosure of PHI and/or ePHI not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410.

F. In accordance with 45 CFR §164.502(e)(1)(ii), require that any subcontractors that create, receive, maintain, transmit or access PHI on behalf of the Contractor agree through contract to the same restrictions and conditions that apply to Contractor with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.

G. Make available to the Secretary, in the time and manner designated by Secretary, Contractor's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County or its users, or created or received by Contractor from or on behalf of County, for purposes of determining, investigating or auditing Contractor's and/or County's compliance with the Privacy Rule. Upon written request and with reasonable notice and time to comply, Contractor will provide relevant copies of its internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County or its users, or created or received by Contractor from or on behalf of County when there is a confirmed breach of PHI or ePHI provided that these copies are treated as Confidential Information.

H. Request, use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure in accordance with 42 USC §17935(b) and 45 CFR §164.502(b)(1).

I. Comply with requirements of satisfactory assurances under 45 CFR §164.512 relating to notice or qualified protective order in response to a third party's subpoena, discovery request, or other lawful process for the disclosure of PHI, which Contractor shall promptly notify County upon Contractor's receipt of such request from a third party, to the extent permitted by law.

J. To the extent this requirement applies, Not require an individual to provide patient authorization for use or disclosure of PHI as a condition for treatment, payment, enrollment in any health plan (including the health plan administered by County), or eligibility of benefits, unless otherwise excepted under 45 CFR §164.508(b)(4) and authorized in writing by County.Use appropriate administrative, technical and physical safeguards to prevent inappropriate use, disclosure, or access of PHI and/or ePHI.

K. Obtain and maintain knowledge of applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.

L. Comply with the requirements of the Privacy Rule that apply to the County to the extent Contractor is to carry out County's obligations under the Privacy Rule.

M. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractor of which Contractor becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Contractor, and if such steps are unsuccessful, Contractor agrees to terminate its contract with the subcontractor if feasible.

6. **Access to PHI, Amendment and Disclosure Accounting.** Contractor agrees to:

A. **Access to, Amendment to, and Accounting of Disclosures of PHI, including ePHI.** If Contractor 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, Contractor shall promptly forward such request to County, to the extent the individual

submitting the request identifies the County as the source of the PHI. Following receipt of such notice from Contractor, County shall be solely responsible for responding to such request and shall not request Contractor's assistance with such request. County acknowledges that as part of its commitment to privacy, Contractor maintains PHI in a manner that does not usually and reasonably permit Contractor to associate the PHI with an individual nor generally with the County, and County 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 Contractor under this BAA, the Underlying Agreement, or any other document or law. Thus, any request from an individual must identify County for Contractor to make such connection to the County and notify County of the request. Otherwise, if the individual does not or cannot identify the County, Contractor will inform the individual making the request that they need to contact their health care provider directly to exercise such rights.

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

7. **Security of ePHI.** In the event County discloses ePHI to Contractor or Contractor needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Contractor shall:

1. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312. For clarity, should Contractor receive any PHI or ePHI outside of the Services either mistakenly or unintentionally by County, Contractor shall make reasonable efforts to detect such PHI or ePHI and provide reasonable security measures to protect the PHI or ePHI and inform the County as soon as reasonably possible for furthering handling and or destruction.

2. Comply with each of the requirements of 45 CFR §164.316 relating to the implementation of policies, procedures and documentation requirements with respect to ePHI, as applicable to Contractor and as required by the Security Rule;

3. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

4. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;

5. Ensure compliance with the Security Rule by Contractor's workforce;

6. In accordance with 45 CFR §164.308(b)(2), require that any subcontractors that create, receive, maintain, transmit, or access ePHI on behalf of Contractor agree through contract to the same restrictions and requirements contained in this Addendum and comply with the applicable requirements of the Security Rule;

7. Report to County any security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,

8. Comply with any additional security requirements that are applicable to covered entities in Title 42 (Public Health and Welfare) of the United States Code, as may be amended from time to time, including but not limited to HITECH.

8. **Breach of Unsecured PHI.** In the case of breach of unsecured PHI, Contractor shall comply with the applicable provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410.

A. **Discovery and notification.** Following the discovery of a breach of unsecured PHI, Contractor shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.

1) **Breaches treated as discovered.** A breach is treated as discovered by Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (determined in accordance with the federal common law of agency).

2) **Content of notification.** The written notification to County relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by Contractor:

a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, used or disclosed during the breach;

b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;

d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

e) A brief description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

B. **Cooperation.** With respect to any breach of unsecured PHI reported by Contractor, Contractor shall cooperate with County and shall provide County with any information requested by County to enable County to fulfill in a timely manner its own reporting and notification obligations, including but not limited to providing notice to individuals, prominent media outlets and the Secretary in accordance with 42 USC §17932 and 45 CFR §164.404, §164.406 and §164.408.

C. **Breach log.** To the extent breach of unsecured PHI involves less than 500 individuals, Contractor shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to County not later than fifteen (15) days after the end of each calendar year for submission to the Secretary.

D. **Delay of notification authorized by law enforcement.** If Contractor delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Contractor shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.

E. **Payment of costs.** With respect to any breach of unsecured PHI caused solely by the Contractor's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, Contractor agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. This provision shall not be construed to limit or diminish Contractor's obligations to indemnify, defend and hold harmless County under Section 9 of this Addendum.

F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor's completed risk assessment and investigation documentation.

G. **Additional State Reporting Requirements.** The parties agree that this Section 8.G applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements

of California Health & Safety Code §1280.15. For purposes of this Section 8.G, "unauthorized" has the meaning given such term in California Health & Safety Code §1280.15(j)(2).

1) Contractor agrees to assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.

2) Contractor agrees to report to County any unlawful or unauthorized access, use, or disclosure of patient's medical information without unreasonable delay and no later than two (2) business days after Contractor determines after reasonable investigation that there has been unauthorized access, use, or disclosure of a patient's medical information. Contractor further agrees such report shall be made in writing, and shall include substantially the same types of information listed above in Section 8.A.2 (Content of Notification) as applicable to the unlawful or unauthorized access, use, or disclosure as defined above in this section, understanding and acknowledging that the term "breach" as used in Section 8.A.2 does not apply to California Health & Safety Code §1280.15.

9. **Hold Harmless/Indemnification.**

A. Contractor agrees to indemnify and hold harmless County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives from any liability whatsoever, based or asserted upon any services of Contractor, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Addendum, including but not limited to property damage, bodily injury, death, or any other element of any kind or nature whatsoever arising from the performance of Contractor, its officers, agents, employees, subcontractors, agents or representatives from this Addendum. Contractor shall defend, at its sole expense, all costs and fees, including but not limited to attorney fees, cost of investigation, defense and settlements or awards, of County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents or representatives in any claim or action based upon such alleged acts or omissions.

B. With respect to any action or claim subject to indemnification herein by Contractor, Contractor shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of County, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of County; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Contractor's indemnification to County as set forth herein. Contractor's obligation to defend, indemnify and hold harmless County shall be subject to County having given Contractor written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Contractor's expense, for the defense or settlement thereof. Contractor's obligation hereunder shall be satisfied when Contractor has provided to County the appropriate form of dismissal relieving County from any liability for the action or claim involved.

C. The specified insurance limits required in the Underlying Agreement of this Addendum shall in no way limit or circumscribe Contractor's obligations to indemnify and hold harmless County herein from third party claims arising from issues of this Addendum.

D. In the event there is conflict between this clause and California Civil Code §2782, this clause shall be interpreted to comply with Civil Code §2782. Such interpretation shall not relieve the Contractor from indemnifying County to the fullest extent allowed by law.

E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Addendum, this indemnification shall only apply to the subject issues included within this Addendum.

10. **Term.** This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by County to Contractor, or created or received by Contractor on behalf of County, is destroyed or returned to County, or,

if it is infeasible to return or destroy PHI and/ePHI, protections are extended to such information, in accordance with section 11.B of this Addendum.

11. **Termination.**

A. **Termination for Breach of Contract.** A breach of any provision of this Addendum by either party shall constitute a material breach of the Underlying Agreement and will provide grounds for terminating this Addendum and the Underlying Agreement with or without an opportunity to cure the breach, notwithstanding any provision in the Underlying Agreement to the contrary. Either party, upon written notice to the other party describing the breach, may take any of the following actions:

1) Terminate the Underlying Agreement and this Addendum, effective immediately, if the other party breaches a material provision of this Addendum.

2) Provide the other party with an opportunity to cure the alleged material breach and in the event the other party fails to cure the breach to the satisfaction of the non-breaching party in a timely manner, the non-breaching party has the right to immediately terminate the Underlying Agreement and this Addendum.

3) If termination of the Underlying Agreement is not feasible, the breaching party, upon the request of the non-breaching party, shall implement, at its own expense, a plan to cure the breach and report regularly on its compliance with such plan to the non-breaching party.

B. **Effect of Termination.**

1) Upon termination of this Addendum, for any reason, Contractor shall return or, if agreed to in writing by County, destroy all PHI and/or ePHI received from County, or created or received by the Contractor on behalf of County, and, in the event of destruction, Contractor shall certify such destruction, in writing, to County. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.

2) In the event that Contractor determines that returning or destroying the PHI and/or ePHI is not feasible, Contractor shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Contractor that return or destruction of PHI and/or ePHI is not feasible, Contractor shall extend the protections of this Addendum to such PHI and/or ePHI and limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as Contractor maintains such PHI and/or ePHI.

12. **General Provisions.**

A. **Retention Period.** Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation consistent with Contractor's product documentation. Customer can export its own information should it need to retain it for longer than the services' native capabilities permit.

B. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.

C. **Survival.** The obligations of Contractor under Sections 3, 5, 6, 7, 8, 9, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.

D. **Regulatory and Statutory References.** A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.

E. **Conflicts.** The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.

F. **Interpretation of Addendum.**

1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.

2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit County to comply with the Privacy Rule, Security Rule, HIPAA and HITECH generally.

G. **Notices to County.** All notifications required to be given by Contractor to County pursuant to the terms of this Addendum shall be made in writing and delivered to the County both by fax and to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Contractor pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer:	HIPAA Privacy Manager
County HIPAA Privacy Officer Address:	26520 Cactus Avenue, Moreno Valley, CA 92555
County HIPAA Privacy Officer Phone Number:	(951) 486-6471
County HIPAA Privacy Fax:	(951) 486-4475

[Intentionally Left Blank; Signature Page Follows]

HIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and CyberArk Software, Inc.

COUNTY OF RIVERSIDE, on behalf of Riverside University Health System

By: _____

Name: V. MANUEL PEREZ

Title: CHAIR, BOARD OF SUPERVISORS

Date: JUN 10 2025

CYBERARK SOFTWARE, INC., a Delaware corporation

Signed by:

By: Natalie Zolnierz
06BD442343DA447...

Name: Natalie Zolnierz

Title: Controller

Date: April 14, 2025

ATTEST:

Kimberly A. Rector

Clerk of the Board

By: _____

Title: DEPUTY

APPROVED AS TO FORM:

Minh C. Tran

County Counsel

By: Esen Sainz

Esen Sainz

Deputy County Counsel

Date: 05/09/2025

JUN 10 2025 18.3