LOGICMONITOR PUBLIC SECTOR MASTER SERVICES AGREEMENT

TABLE 1 - GENERAL INFORMATION

Purpose	Contract for Subscription Services (SaaS) (defined below)
Auto-Renewal (Y/N)	No / Not Applicable
Cust. Software Dev.	None / Not Applicable
Support	Included with subscription (advanced tiers available). Maintenance not separate.
Vendor	LogicMonitor, Inc.
Vendor Address	820 State St., 5th Floor, Santa Barbara, CA 93101 U.S.A.

TABLE 2 - DOCUMENT LIST

Exhibit	Description
Exhibit A	Information Security and Privacy
Exhibit B	Service Level Terms
Exhibit C	Technical Support Exhibit
Exhibit D	Data Protection Addendum (DPA)
Exhibit E	Background Checks
Exhibit F	Operational Resiliency

1. AGREEMENT.

This Public Sector Master Services Agreement (these "Terms" or this "Agreement") is entered into as of the last date of signature on the Order Form or this Agreement (the "Effective Date"), by and between LogicMonitor, Inc., a Delaware corporation having its headquarters at 820 State St., 5th Floor, Santa Barbara, CA 93101 U.S.A. (below referred to as "LogicMonitor," "we," "our", "us" or "Company") and the corporation or other legal entity set forth on the Order Form (below referred to as "Customer", "you" or "your"), and will govern the use of the LogicMonitor hosted data center monitoring services (the "Service" or "Services") and any associated use of the LogicMonitor Technology offered by LogicMonitor, Inc. Customer and LogicMonitor are sometimes hereinafter referred to individually as a "party" and collectively as the "parties".

2. YOUR SUBSCRIPTION.

A. We offer subscription-based Services. By subscribing to the Services, you have a limited, non-exclusive, royalty-free (apart from the Services fees due to LogicMonitor), non-transferable and terminable license to access and to use the Services solely for your internal business operations during your subscription period specified on the applicable order form through which the Services are ordered (each an "Order Form"). You are expressly prohibited from sublicensing use of the Services to third parties. However, you may choose to offer access to and use of the Services to your Affiliates, provided that (i) you shall remain the contracting party with us with respect to the payment of fees and all access and use; and (ii) you hereby agree that you shall retain full, unconditional responsibility for all such access to and use of the Services and LogicMonitor Technology and all compliance herewith. "Affiliate" means a corporation or other legal entity which a party owns or controls, is controlled by or is under common control with such entity through ownership or control of more than 50% of the shares entitled to vote. You hereby agree that neither you nor your Affiliates or customers shall take any action intended to interfere with or disrupt the Services or any other user's use of the Services.

B. Support. LogicMonitor will provide any technical support included with your subscription purchase in accordance with the terms of your applicable support plan, as described at https://www.logicmonitor.com/legal/technical-support-exhibit. Customer will automatically be enrolled in the

basic support plan at no additional charge. Premier support plans are available for purchase and, if applicable, will be set forth on your Order Form.

C. We shall use commercially reasonable efforts to make the Services available 24 hours a day, 7 days a week during the Term, except for:

(i) Planned Maintenance. "Planned Maintenance" means maintenance where at least forty-eight (48) hours prior notice is provided via email based on your account settings within the Services, or by using Notification capabilities within the Services (see https://support.logicmonitor.com/). Planned Maintenance shall be conducted only during the hours of 6:00p.m. to 12:00a.m. Pacific Time and shall not exceed (a) 8 hours in any given month, or (b) 40 hours in any given year. Downtime will be minimized at all times and if the expected impact of planned operations is less than five (5) minutes of downtime, we may elect not to give advance notice; or

(ii) Extraordinary Circumstances. "Extraordinary Circumstances" means any unavailability caused by circumstances beyond our reasonable control, including without limitation, acts of God, acts of government (including U.S. sanctions or embargoes), flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems, or Internet outages or delays.

D. Your use of the Services is expressly only licensed for the duration of the Term and any trial period while you are and remain a current customer in good standing. You acknowledge and agree that you will not have access to historical information or data related to your use of the Services upon expiration or termination of your use of the Services; provided, however, that we agree to assist upon your request prior to termination to download all such available data.

E. Professional Services. Professional Services may be included in your Order Form upon request. Fees, coverage and terms for Professional Services are available from LogicMonitor and will be set forth on your Order Form and/or a separate statement of work for such Professional Services. "Professional Services" means services provided by LogicMonitor personnel on a time and materials or fixed price basis for a customer-identified project or scope of work.

F. Beta Services. LogicMonitor may make certain features or functionality available in a controlled beta test, private preview, or similar specially designated program ("Beta Program") involving pre-release features or functionality that may be subject to change, or discontinuation ("Beta Test"). Free Beta Test product(s) are provided on an early release basis, and are not intended to function as a generally available offering, subject to the applicable Beta Program rules.

3. SUBSCRIPTION FEES, BILLING AND RENEWAL.

A. Paid Subscription. By subscribing to the Services, you expressly agree to pay subscription fees corresponding to your subscription plan, plus any applicable taxes and duties, if any. Annual subscription fees are fully earned upon payment and, except as otherwise specified herein, the payments are nonrefundable and there are no refunds or credits for partial subscription periods. Subscription fees are fully earned upon payment and, except as otherwise specified herein, the payments are nonrefundable and there are no refunds or credits for partial subscription periods.

(i) Your Subscription. Except as otherwise set forth on your Order Form for the Services, fees are billed as of the Service commencement date for the entire initial subscription period set forth on the Order Form (the "Initial Term") and for each additional renewal period of the same length (a "Renewal Term"), for the initial quantity commitment specified in the Order Form (the "Reserved Commitment"), net of any contractual discount. The period of your use of the Services during the Initial Term and each Renewal Term under this Agreement is referred to as the "Term".

(ii) Any increase in the actual usage beyond the Reserved Commitment will be billed to you by LogicMonitor for each month of Service, upon the end of the applicable month, via invoice at the applicable overage pricing rate set forth on your Order Form. Such invoiced amounts, if applicable, shall be due and payable in accordance with this Agreement. Usage of the Service is calculated in accordance with the methodology set forth below.

A1. No Overages for Public Sector Entities. In consideration of Customer's status as a government or public sector entity, LogicMonitor agrees to waive any charges incurred during the initial year of the subscription Term that arise from Customer exceeding the committed quantities specified in the applicable subscription. This is provided that Customer acknowledges and agrees that any waived fees shall constitute actual, truthful cost or usage data pursuant to applicable laws and regulations, and that the inclusion of these costs in the consideration for pricing for any subsequent year(s) or subscription renewal is fair and reasonable in the ordinary course of business. For clarity, the foregoing will not apply in the event that overages are not applicable to the specific Service in question. In this event, the parties will specify such in the applicable Order Form.

B. Usage. Your usage of the Service is measured on a calendar month basis. For purposes of measuring usage, a "host" or "device" is a logical host defined by a network (IP) address, physical, virtual, or cloud. Host or device usage is measured by the average over a month. Specific LogicMonitor services such as Edwin AI, Logs, and APM are measured in terms of the total usage over a calendar month. Overage fees shall only apply if usage for a month exceeds the Reserved Commitment.

C.Reserved. .

D. When Payments are Due. All payments shall be due and payable as described in the applicable Order Form (the "due date"). LogicMonitor or its authorized reseller as applicable shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k). Late payments will be subject to late fees at the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid..

4. TERM AND TERMINATION. This Agreement is in force from the Effective Date (or, if earlier, the first date of your use of the Services or Software) and, subject to any earlier termination permitted in this Agreement, will remain in force throughout the Term. Except where your early termination is pursuant to LogicMonitor's uncured material breach (pursuant to subsection (A) below) (in which case we will promptly refund to you the prepaid fees (if any) for that portion of the terminated period for which Services were not provided), early termination of a subscription or ceasing your use of the Services will not result in a refund of any annual prepaid fees. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, LogicMonitor shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Additionally, immediately upon the detection of suspicious circumstances or behavior, or the receipt of information we believe is credible regarding the unauthorized use or disclosure of your data or of a demonstrable threat to either your data or the LogicMonitor Technology, LogicMonitor has the right to temporarily suspend the access to or use of the Service or LogicMonitor Technology by your authorized users. In such event, we will provide a prompt, written description of the issue(s) or event(s) resulting in the suspension, and you agree to regularly communicate with our support team, and work in good faith to resolve the matter promptly. For the avoidance of doubt, we are not responsible for, and termination under this Section will not apply when any delay in restoration of services is related to your failure to provide prompt responses, reasonable assistance, and cooperation with us.

5. OUR TECHNOLOGY.

A. The Services are enabled by and utilize a hosted software application (the "LogicMonitor Software"). We shall host the LogicMonitor Software and may update the functionality and user interface of the LogicMonitor Software from time to time in our sole discretion as part of our ongoing mission to improve the Services and our users' use of the Services, provided that such modifications will not materially decrease the functionality of the Services. You must have access to the LogicMonitor Software in order to use the Services. In addition, to use the Services fully, you will be required to download and install a piece of our software on your network (the "Collector Software" and collectively with the LogicMonitor Software, the "Software").

B. You agree that the rights granted to you are provided on the condition that you will not (and will not allow, give permission to or enable any third party, including without limitation any customer or Affiliate, to) copy, create a Derivative Work of, or reverse engineer, reverse assemble, disassemble, or decompile the Software or any part thereof or otherwise attempt to discover any source code, modify the Software in any manner or form, or use unauthorized modified versions of the Software, including (without limitation) for the purpose of building a similar or competitive product or service or for the purpose of obtaining unauthorized access to the Services. "Derivative Work" means any modification of or extension to any software, process, algorithm, trade secret, work of authorship, invention, or to any other intellectual property right therein or thereto.

C. License. Subject to your compliance with the terms of this Agreement, we hereby grant to you a limited, non-exclusive, royalty-free (apart from the fees paid to LogicMonitor for the Services), non-transferable license to download, install and use the Collector Software (in object code form) onto your network for internal business purposes for the sole purpose of using the LogicMonitor Service. The Software is not sold but licensed hereunder.

6. OWNERSHIP.

A. LogicMonitor Technology. You acknowledge and agree that the LogicMonitor Software, including the specific design and structure of individual programs, components and aspects thereof, constitutes the proprietary trade secrets and copyrighted material of LogicMonitor, and that LogicMonitor owns all rights, title and interest in and to the Services, the Software, Feedback and all technology, information, trade secrets, patent rights, copyrights, know-how and documentation associated therewith as provided or otherwise made available by LogicMonitor and used in the performance of the Services, including all intellectual property rights and Derivative Works therein, on a worldwide basis (collectively, the "LogicMonitor Technology"). As used herein, "Feedback" means bug reports, suggestions, comments or other feedback provided by Customer to LogicMonitor with respect to the Service, excluding any Customer Confidential Information. The license granted to you is limited by these Terms and does not convey any other rights in the LogicMonitor Technology, express or implied, nor does it grant any ownership in the LogicMonitor Technology or any intellectual property rights therein or thereto. Any rights not expressly granted herein are reserved by LogicMonitor.

B. Customer Data. You retain all right, title and interest in and to all Customer Data. "Customer Data" means electronic data, files or information submitted by Customer to the Service. LogicMonitor's right to access and use Customer Data is limited to the right to access and use such Customer Data for the purpose of providing the Service or as may otherwise be explicitly set forth in this Agreement. No other rights with respect to your Customer Data are implied. Customer Data shall at all times be classified and treated as Confidential Information hereunder.

C. Implementations. Excluding your Confidential Information, and any applicable Personal Data, you agree that if you make any customizations or customized implementations of the Software or LogicMonitor Technology that do not qualify as Derivative Works ("Implementations"), such Implementations are hereby licensed to us on a non-confidential, nonexclusive, irrevocable, worldwide, royalty-free, sublicensable basis to perform services, use, distribute, publish, display, copy, sell, have sold, make, have made, create Derivative Works of, import, export, and license the Implementations and products and services utilizing or incorporating the Implementations, and to otherwise commercially exploit the same. If any integrations with third party tools,

platforms or programs are implemented for your use in conjunction with the Service, you agree that LogicMonitor has no obligation to support the same.

D. Copyright and Proprietary Legends. You agree not to remove any copyright or proprietary legends in the LogicMonitor Technology, and to implement reasonable security measures to protect our proprietary rights therein from unauthorized use or disclosure. Certain marks, words and logos displayed on the Services, which may or may not be designated by a "™" "®" "SM" or other similar designation, constitute trademarks, trade names, or service marks belonging to us or our licensors. Except as necessary for you to make use of the Services in accordance with the license rights herein, you are not authorized to use any such marks. Ownership of all such marks and the goodwill associated therewith remains with us or our respective licensors.

7. CONFIDENTIALITY.

A. The parties agree that during the course of performance under these Terms, each party may disclose to the other party certain technical and/or non-technical information, which (i) is disclosed in a tangible or visual form and clearly labeled as "Confidential"; (ii) is disclosed in an oral, non-tangible or visual form, identified at the time of disclosure as confidential and confirmed in writing within thirty (30) days; or (iii) is identified and treated as confidential by disclosing party and given the circumstances of disclosure, and/or the nature of the information, the recipient knew or should reasonably have known the information was confidential (collectively, the "Confidential Information"). For purposes of clarification and in addition to the Confidential Information addressed in the previous sentence, LogicMonitor Technology shall be deemed our Confidential Information and all Customer Data shall be deemed your Confidential Information. Confidential Information does not include information, technical data or know-how which (a) is rightfully in the possession of the receiving party at the time of disclosure as shown by the receiving party's files and records immediately prior to the time of disclosure; (b) prior to or after the time of disclosure becomes part of the public knowledge or literature, not as a result of any inaction or action of the receiving party; (c) is approved in writing for release by the disclosing party; or (d) is independently developed by the receiving party without use of or reference to any Confidential Information of the disclosing party.

B. Each party agrees not to use the Confidential Information disclosed to it by the other party for any purpose except as necessary to perform its obligations under these Terms. Neither party will disclose the Confidential Information of the other party to third parties or to the first party's employees except employees and service providers who are required to have the information in order to carry out such party's obligations hereunder who have agreed in writing, as a condition of employment, engagement or otherwise (or who are otherwise bound by fiduciary duty or rules of professional conduct), to protect the Confidential Information with terms no less stringent than are imposed by this Section; provided, however, that this Agreement may also be disclosed to potential successors in interest (and their respective attorneys and advisors) pursuant to a contemplated merger, acquisition, corporate reorganization or sale of all or substantially all of a party's assets, so long as such recipient in each case has agreed in writing to protect the Confidential Information with terms no less stringent than are imposed by this Section. Notwithstanding the above, LogicMonitor may use data about Customer's configuration and use of the Service that has been aggregated and/or anonymized (collectively, "Usage Data") in order to (i) measure general Service usage patterns and characteristics of its user base and/or (ii) to improve the Service and develop new insights and features, and may include such Usage Data in promotional materials or reports to third parties; provided, that, for the avoidance of doubt, (x) such Usage Data is rendered in such a manner that does not allow a third party to identify Customer or its suppliers, customers, contractors, agents, affiliates, or subsidiaries and (y) such Usage Data does not reference Personal Data, names, phone numbers, email addresses, or other personally identifiable information. "Personal Data" generally means nonpublic, personally identifiable information of or concerning any living individual among the consumers, employees, clients and customers of Customer or LogicMonitor, their parents, subsidiaries, affiliates and agents. Each party agrees that it will use the same standard of care that it uses in protecting its own Confidential Information, but in no case less than reasonable care. Each party agrees to promptly notify the other in writing of any misuse or misappropriation of Confidential Information of the other party that may come to its attention.

C. The confidentiality and non-use obligations of each receiving party under this Agreement will survive expiration or termination of this Agreement for a period of five (5) years; except that such obligations shall survive indefinitely with respect to (i) Personal Data, and (ii) each disclosing party's software and technology-based trade secrets so long as they remain eligible for trade secret under prevailing law (without regard to any breach of the receiving party). In the event of any expiration or termination of these Terms, or upon request by the disclosing party, the receiving party shall cease all use of the other party's Confidential Information and return to the disclosing party all copies of the disclosing party's Confidential Information in the receiving party's possession or control, or destroy the same and certify as to its destruction. The receiving party will not be required to return or immediately destroy an archive copy of the disclosing party's Confidential Information made for backup purposes in the ordinary course; provided that such archive copy will be subject to the ongoing obligations of confidentiality and non-use contained herein and shall be destroyed in the ordinary course of business not to exceed ninety (90) days, or with respect to Personal Data, such shorter period as is necessary to comply with prevailing law.

D. While the parties understand that incidental capturing of certain nominal Personal Data may occur in connection with the Service (as described in the DPA), the purpose and focus of the Service is on IT systems performance monitoring and not to function as a receptacle or conduit to store, manipulate, transmit or retrieve Restricted Data. As used herein, "Restricted Data" means (i) Protected Health Information, as such term is defined under the U.S. Health Insurance Portability and Accountability Act, (ii) financial account data or payment cardholder information under PCI Data Security Standard, (iii) Personal Data beyond that which is incidental to the Service and described in the DPA, and/or (iv) any other data that is subject to specific or heightened requirements under applicable law or industry standards, such as Social Security numbers in the United States. Without limiting its other obligations under this Agreement, and subject to the foregoing caveat regarding collection of certain nominal Personal Data, the parties agree that (x) you shall not provide Restricted Data to LogicMonitor, and shall configure the Collector Software so that it will be used only to collect information from devices and applications using methodology which will not expose or divulge Restricted Data; (y) you will not send any logs to LogicMonitor that contain Restricted Data; and (z) you will isolate and secure the Software on your systems and network to prevent unauthorized access, use, disclosure and loss using at a minimum industry standard security practices and technologies and as otherwise required by applicable laws.

E. Compelled Disclosure. In the event that the receiving party is required by applicable law, regulation or any competent judicial, supervisory or regulatory body to disclose any of the Confidential Information, the receiving party shall provide the disclosing party with prompt written notice of any such requirement so that the disclosing party may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. If, however in the opinion of the counsel of the receiving party, the receiving party is nonetheless, in the absence of such order or waiver, compelled to disclose such Confidential Information, then it may disclose only such portion of the Confidential Information which, in the opinion of its counsel, the receiving party is compelled to disclose. The receiving party will not oppose any action by the disclosing party to obtain reliable assurance that confidential treatment will be accorded the Confidential Information. The receiving party will reasonably cooperate with the disclosing party in its efforts to obtain a protective order or other appropriate remedy that the disclosing party elects to seek to obtain, in its sole discretion. LogicMonitor recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

F. Each party shall comply with prevailing laws and regulations governing Personal Data, including, without limitation and as may be applicable, the EU General Data Protection Regulation ("GDPR"), the UK General Data Protection Regulation ("UK GDPR"), the California Consumer Privacy Act ("CCPA"), and the California Privacy Rights Act ("CPRA"). If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not

agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

G. Service Provider Attestation (CCPA/CPRA). LogicMonitor is a "Service Provider" as defined under the CCPA and CPRA. Customer discloses Personal Data (as defined under the CCPA and CPRA) to LogicMonitor solely (i) for a valid business purpose and (ii) for LogicMonitor to provide the Services contemplated by this Agreement. LogicMonitor expressly certifies, understands and agrees that except as permitted or required by applicable law, it is prohibited from (1) selling (as defined under the CCPA and CPRA) any of Customer's Personal Data, (2) retaining, using or disclosing any of Customer's Personal Data for any commercial purpose other than providing the Services contemplated by this Agreement, (3) retaining, using or disclosing Personal Data outside of the direct business relationship between LogicMonitor and Customer and this Agreement, or (4) combining the personal information that it receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that LogicMonitor may combine personal information to perform a business purpose in limited circumstances. LogicMonitor understands the prohibitions that are outlined in this Section 7(G) and hereby certifies its compliance therewith. LogicMonitor shall generally not respond to end user requests except to the extent required by law, and shall direct such requests to Customer where feasible. We will notify you in the event that we cannot meet our obligations as a Service Provider under the CCPA, CPRA, and applicable regulations. We will also provide any required information to enable you to comply with a consumer request, if applicable.

H. Data Processing Addendum. The parties hereby agree to comply with the terms of the Data Processing Addendum attached hereto as Exhibit D (the "DPA").

I. Security Practices. During the Term, LogicMonitor will implement and maintain administrative, physical and technical safeguards and measures designed to protect against unauthorized access to Customer Data as more fully described here: https://www.logicmonitor.com/security-practices ("Security Practices"). During the Term, LogicMonitor will not materially diminish the protections provided by the Security Practices.

K. Penetration Testing. LogicMonitor performs annual penetration testing on the Service ("Pen Test"). A Pen Test is a simulated attack that may include tools, techniques, and processes to identify vulnerabilities and weaknesses in a computer system, application, service, or environment, that is part of delivery of the Services. You may not conduct any Pen Test without advanced notice, express written consent, and authorization from LogicMonitor. You, not LogicMonitor, are responsible for any resulting issue(s) caused by your Pen Test performed in violation of these restrictions.

8. REPRESENTATIONS AND WARRANTIES.

A. Representations. Each party hereby represents and warrants to the other that (i) such party has the right, power and authority to enter into these Terms and to fully perform all its obligations hereunder; and (ii) the making of these Terms does not violate any agreement existing between such party and any third party.

B. Limited Service Warranty.

(i) We warrant that we will deliver and perform the Services in a good and workmanlike manner consistent with applicable industry standards and the functional requirements and technical specifications set forth in the applicable Order Form.

(ii) Service Level Terms. We will provide the Services in accordance with the service level terms attached hereto as Exhibit B(individually or collectively, the "Service Level Terms"), and any remedies for failure to comply with such standards are set forth therein.

C. In the event that Customer notifies LogicMonitor in writing of a breach of the foregoing warranties, LogicMonitor shall use commercially reasonable efforts to correct the reported non-conformity, at no additional charge to Customer, or if LogicMonitor determines such remedy to be impracticable, Customer may terminate this Agreement and receive a prorated refund of fees pre-paid to LogicMonitor for Customer's use

of the Service for the remainder of the then current subscription period. The foregoing remedy shall be Customer's sole and exclusive remedy for any breach of warranty hereunder; provided, that, remedies available for breach of the Service Level Terms are as set forth in the Service Level Terms.

9. INDEMNIFICATION.

A. By LogicMonitor. We shall, at our own expense, indemnify, have the right to intervene to defend and hold you harmless from and against any damages and expenses (including reasonable attorneys' fees) as a result of third party claims, to the extent of any finding that the LogicMonitor Technology, when used in strict compliance with the license rights and use instructions provided by LogicMonitor infringed or misappropriated the intellectual property right(s) of a third party; provided we receive prompt notice and the opportunity to provide the defense and participate in the litigation and settlement negotiations. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. Notwithstanding the foregoing, we shall have no liability, and shall have no obligation to defend or indemnify you, for any third party claim of infringement to the extent based upon (i) use of other than the then current, unaltered version of the LogicMonitor Technology and applicable Services, unless the infringing portion is also in the then current, unaltered release; (ii) use of the Services or LogicMonitor Technology other than strictly in accordance with our instructions and documentation; or (iii) use, operation or combination of the applicable Services with non-LogicMonitor programs, data, equipment or documentation if such infringement would have been avoided but for such use, operation or combination. In the event the use of any Service or LogicMonitor Technology is, or we believe is likely to be, alleged or held to infringe any third party intellectual property right, we may, at our sole option and expense, (a) procure for you the right to continue using the affected service, (b) replace or modify the affected service with functionally equivalent service so that it does not infringe, or, if either (a) or (b) is not commercially feasible, (c) terminate the Services and refund the fees received by us from you for the affected service for the remaining Term of then-current subscription period. THE FOREGOING CONSTITUTES OUR ENTIRE LIABILITY, AND YOUR SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY THIRD PARTY CLAIMS OF INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OF ANY KIND OR NATURE.

B. [RESERVED].

10. DISCLAIMERS, LIMITATION OF DAMAGES AND LIABILITY.

A. DISCLAIMERS AND EXCLUSIVE REMEDY.

EXCEPT FOR THE REPRESENTATIONS AND LIMITED WARRANTY IN SECTIONS 8.A (REPRESENTATIONS) AND 8.B. (LIMITED SERVICE WARRANTY), THE SERVICES AND LOGICMONITOR TECHNOLOGY ARE PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED OR ANY WARRANTIES ARISING FROM A COURSE OF DEALING OR TRADE USAGE INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE, NOR DO WE WARRANT THAT THE LOGICMONITOR TECHNOLOGY OR SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR REGARDING THE SECURITY, ACCURACY, RELIABILITY, TIMELINESS OR PERFORMANCE OF THE SERVICES. WE MAKE NO WARRANTY ABOUT THE SUITABILITY OF THE LOGICMONITOR TECHNOLOGY OR SERVICES FOR ANY PURPOSE AND DO NOT WARRANT THAT THE LOGICMONITOR TECHNOLOGY OR SERVICES WILL MEET YOUR REQUIREMENTS.

CUSTOMER ACKNOWLEDGES AND AGREES THAT LOGICMONITOR SHALL NOT HAVE ANY LIABILITY FOR (I) MODIFICATIONS OR ALTERATIONS TO THE COLLECTOR SOFTWARE MADE BY YOU OR ANY THIRD PARTY NOT AUTHORIZED BY LOGICMONITOR OR (II) CUSTOMER'S USE OF MONITORING SCRIPTS MADE AVAILABLE IN LM EXCHANGE, LOGICMONITOR'S CUSTOMER COMMUNITY, THAT ARE NOT AUTHORED BY LOGICMONITOR. IN ADDITION, ANY SOFTWARE INTENDED TO ASSIST IN ESTIMATING THE COST OR SIZE AND

SCOPING OF A CUSTOMER'S NETWORK OR INFRASTRUCTURE IS NOT INTENDED AS A SUBSTITUTE FOR PROFESSIONAL FINANCIAL ADVICE; THE SOFTWARE IS ENTIRELY DEPENDENT ON CUSTOMER-PROVIDED INPUT(S) AND CUSTOMER'S EXPERTISE.

B. INDIRECT AND CONSEQUENTIAL DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCLUDING THE INDEMNIFICATION OBLIGATIONS IN SECTION 9 OR CLAIMS, LIABILITIES OR LOSSES ARISING FROM FRAUD OR INTENTIONAL MISCONDUCT, OR GROSS NEGLIGENCE, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES ARISING OUT OF OR IN ANY WAY RELATING TO THESE TERMS, THE SERVICES PROVIDED, OR THE USE OF OR INABILITY TO USE THE SERVICES INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, LOST PROFITS, LOSS OF DATA, COMPUTER FAILURE OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES EVEN IF ADVISED OF THE POSSIBILITY THEREOF AND REGARDLESS OF THE LEGAL OR EQUITABLE THEORY (CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE) UPON WHICH THE CLAIM IS BASED.

C. LIMITATION OF LIABILITY. EXCEPT WITH RESPECT TO LIABILITIES OR LOSSES ARISING FROM FRAUD OR INTENTIONAL MISCONDUCT, OR GROSS NEGLIGENCE, IN NO EVENT WILL EITHER PARTY'S AGGREGATE, CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THESE TERMS AND ALL ORDER FORMS EXCEED (I) THE SUM OF THE AMOUNTS RECEIVED BY AND OWED TO US FROM YOU DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY, AND (II) TWO (2) TIMES THE AMOUNT IN SUBSECTION (I) WITH RESPECT TO A PARTY'S INDEMNITY OBLIGATIONS UNDER ARTICLE 9 OR LIABILITIES OR LOSSES RESULTING FROM EITHER PARTY'S BREACH OF ITS OBLIGATIONS UNDER ARTICLE 7 (CONFIDENTIALITY), WHICH FOR CLARITY, INCLUDES ALL DATA PRIVACY AND INFORMATION SECURITY OBLIGATIONS. THESE LIMITATIONS ARE CUMULATIVE FOR ALL CLAIMS HOWSOEVER ARISING UNDER ALL AGREEMENTS AND ORDERING DOCUMENTS, AND SHALL APPLY EVEN IF THE REMEDIES PROVIDED IN THIS AGREEMENT SHALL FAIL OF THEIR ESSENTIAL PURPOSE. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) BODILY INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

D. BASIS OF BARGAIN. YOU ACKNOWLEDGE AND AGREE THAT THE FOREGOING SECTIONS ON WARRANTIES AND DISCLAIMERS, INDEMNIFICATION AND LIMITATION OF LIABILITY FAIRLY ALLOCATE THE RISKS BETWEEN THE PARTIES AND ARE ESSENTIAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. YOU EXPRESSLY ACKNOWLEDGE THAT THE FEES THAT WE CHARGE FOR THE SERVICES ARE BASED UPON OUR EXPECTATION THAT THE RISK OF ANY LOSS OR INJURY THAT MAY BE INCURRED BY USE OF THE SERVICES WILL BE BORNE BY YOU AND NOT US AND WERE WE TO ASSUME ANY FURTHER LIABILITY OTHER THAN AS SET FORTH HEREIN, SUCH FEES WOULD OF NECESSITY BE SET SUBSTANTIALLY HIGHER.

11. GENERAL PROVISIONS.

A. Notices. You agree to provide LogicMonitor with your email address, to promptly provide LogicMonitor with any changes to your email address, and to accept emails (or other electronic communications) from LogicMonitor at the email address you specify. Except as otherwise provided in this Agreement, you further agree that LogicMonitor may provide any and all notices, statements, and other communications to you through either email or posting on the Service portal. Notices to you may be provided by email and shall be addressed to the system administrator or user designated by you for your relevant Services account, and in the case of billing-related notices, to the relevant billing contact designated by you. The Company maintains the right to require placement of a valid email address within the Services portal for both billing, Services notification and notices purposes. In no event shall the Company be held liable for negative

consequences resulting from a lack of Company notices in the case notification email addresses are not included by you in the Services portal as required. Legal notices to you may at our option also be sent to the address on the Order Form or that you have last provided, and such notices to us should be sent to LogicMonitor, Inc., 820 State St. 5th Floor, Santa Barbara, CA 93101, USA, Attention: Legal Department or by email to legal@logicmonitor.com.

B. Governing Law, Jurisdiction and Dispute Resolution. If Customer is a public sector agency, state or local government, or similar public entity, the parties agree to the Federal law of the United States.

C. Notice to U.S. Government Users. All LogicMonitor products and services are commercial in nature. The Software and LogicMonitor Technology are "Commercial Items," as defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are licensed to U.S. Government end users (i) only as Commercial Items, and (ii) with only those rights as are granted to other users pursuant to these Terms. All unpublished rights are reserved.

D. Export Restrictions. Each party shall (i) comply with applicable laws and regulations administered by the U.S. Commerce Bureau of Industry and Security, U.S. Treasury Office of Foreign Assets Control or other governmental entity imposing export controls and trade sanctions ("Export Restrictions"), including designating countries, entities and persons ("Sanctions Targets") and (ii) not directly or indirectly export, re-export or otherwise deliver Services to a Sanctions Target, or broker, finance or otherwise facilitate any transaction in violation of any Export Laws. Customer represents that it is not a Sanctions Target or prohibited from receiving Services pursuant to this Agreement under any applicable laws or regulations, including Export Restrictions. LogicMonitor products and services may not be used, accessed, exported, re-exported, or otherwise made available in or to any individual, entity, or organization located in the following regions: China, Hong Kong, Russia, and any country or territory subject to comprehensive sanctions or trade restrictions under applicable U.S., UK, EU, or other relevant laws (including, but not limited to, Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine). Further, the parties agree that the Services may not be used in furtherance of the provision of products or services to any entity that is restricted or otherwise sanctioned by the United States Department of Commerce, nor any entity on the U.S. Federal Communications Commission's "Covered List," nor any Covered Application, as described in the United States Consolidated Appropriations Act, 2023.

E. Anti-Bribery and Anti-Corruption. LogicMonitor is committed to conducting business that is free from any and all forms of corruption or bribery, including kickbacks, money laundering and fraud. LogicMonitor is committed to compliance with all applicable anti-bribery and anti-corruption laws and regulations, including but not limited to the U.S Foreign Corrupt Practices Act 1977 and the UK Bribery Act 2010. Each party agrees not to directly or indirectly offer, promise, provide or accept anything of value to or from the other party's employee, a government official or commercial business partner in violation of any provisions of any applicable anti-bribery laws in connection with this Agreement or any LogicMonitor business.

LogicMonitor shall ensure that it is, and all of its personnel and affiliates are, in full compliance with the UK Modern Slavery Act 2015.

F. High Risk Activities. The Software is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). The Company specifically disclaims any express or implied warranty of fitness for High Risk Activities.

G. Severability. If any provision of these Terms is held by a court of competent jurisdiction to be unenforceable or contrary to law, the provision shall be modified by the court and interpreted so as best to

accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of these Terms shall remain in effect.

H. Insurance. LogicMonitor will, at its expense, during the Term and for the 2-year period following termination or expiration hereof, purchase and maintain insurance policies with an insurance company or companies of U.S. or internationally-recognized standing with a rating of A-/Class IX, or better, as rated by A.M. Best, with the following minimum limits:

(i) Comprehensive General Liability Insurance, with limits not less than $1,000,000 per occurrence and $2,000,000 in the aggregate, covering bodily injury, personal injury and property damage;

(ii) Technology Errors and Omissions Insurance, with limits of not less than $1,000,000 per claim and $1,000,000 in the aggregate with respect to claims related to the LogicMonitor Technology delivered by LogicMonitor under this Agreement;

(iii) Privacy and network security liability ("Cyber") Insurance, with limits of at least $1,000,000 per claim and $2,000,000 in the aggregate, providing protection against liability for privacy breaches, system breaches, denial or loss of service, introduction, implantation or spread of malicious software code and unauthorized access to or use of computer systems; and

(iv) Workers Compensation and Employers Liability Insurance as required by applicable laws, in amounts that meet or exceed those required by applicable laws.

If any of such insurance policies are to be modified or canceled during the Term of this Agreement in a way that would materially affect the coverage required hereunder, LogicMonitor will provide written notice to Customer at least thirty (30) days prior to such modification or cancellation. Each party will, upon a party's request, provide the other party with certificates of insurance evidencing satisfactory coverage of the types and limits set forth above.

I. Survival. Sections 3 (Subscription Fees, Billing and Renewal) (surviving until all fees and charges are paid), 4 (Term and Termination), 5.B. (Our Technology), 6 (Ownership), 7 (Confidentiality) (surviving for the term specified therein), 9.B. (Indemnification), 10 (Disclaimers, Limitation of Damages and Liability), and 11 (General Provisions) (surviving according to the specified periods, if any), shall survive expiration or termination of this Agreement.

J. Third-Party Programs. Customer may receive access to third-party software programs ("Third-Party Programs") through the Collector Software, and/or third-party programs may be bundled with the Collector Software. These Third-Party Programs are governed by their own license terms, which may include open source licenses, and those terms will prevail over the terms of this Agreement as it relates to Customer's use of Third-Party Programs. This Agreement does not limit Customer's rights under any such Third-Party Program or grant Customer any rights that supersede the terms of any such license agreement for a Third-Party Program.

K. Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld). Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

L. Publicity.

(i) Neither party will make any news or press release regarding this Agreement without the other party's prior written consent. You grant us the right to include your name as a customer in our promotional materials to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71; provided however, that you can opt to have your name excluded from such use by us except as agreed to in writing on a case-by-case basis by providing a sufficiently detailed email request

regarding the same to customer-marketing@logicmonitor.com; the subject line in such email should be entitled "Non-use of Subscriber Name."

(ii) Subject in each case to your agreement and only on an occasional basis, we may ask that you consider in your sole discretion making a representative available (x) to serve as a non-public reference to our prospective customers to discuss your experience working with us; and (y) to work with us in developing and publishing case studies and press releases that describe your use of the Services.

M. Force Majeure. In accordance with GSAR Clause 552.212-4(f), Except for the nonpayment of money due, neither party shall be liable for any delay or failure in performance due to Extraordinary Circumstances (as defined in Section 2.C.(ii) hereof).

N. Effect of Transaction. For the avoidance of doubt, (i) in the event that Customer is acquired by or merged into another entity that is a customer of LogicMonitor, this Agreement and the commercial terms set forth on any Order Form hereunder shall continue to apply for the subscription term set forth on any such Order Form; and (ii) in the event that Customer acquires (whether by acquisition or merger) another entity that is a customer of LogicMonitor, Customer acknowledges and agrees that the commercial and legal terms then in place between LogicMonitor and such entity shall continue for the duration of such entity's current subscription term.

O. Compliance with Federal, State and Local Laws. Each party agrees the Services provided hereunder shall be delivered and used in accordance with all applicable federal, state and local laws and regulations.

P. Relationship of the Parties. The parties are independent contractors and this Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the parties. There are no third-party beneficiaries to this Agreement.

Q. Waiver and Cumulative Remedies. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies available to a party at law or in equity.

R. Entire Agreement. This Agreement and any attachments approved by the parties hereto along with any Order Forms constitute the entire agreement between the parties and supersede all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter, including but not limited to any non-disclosure and proof of concept agreements entered by the parties and any click-through or online terms. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and either signed or accepted electronically by the party against whom the modification, amendment or waiver is to be asserted. In addition, purchase orders are used for convenience of ordering only, and no purchase order terms and conditions will supplement this Agreement. In the event of any conflict or inconsistency between the provisions of this Agreement and any Order Form, the same shall be resolved by giving precedence to this Agreement.

The Parties agree by signing below:

CUSTOMER:	**LOGICMONITOR, INC.**
By:	By:

Name:	Name:
Title:	Title:
Email:	Email:
Date:	Date:

«Close##SignatureBlockSpan»

[***Exhibits Follow***]

Exhibit A

Information Security and Privacy

1. Purpose

This Security Exhibit outlines the essential security and privacy practices LogicMonitor shall meet and maintain in order to fulfill its obligations under the terms of the Agreement.

LogicMonitor may update or modify these practices from time to time, provided such updates and modifications shall not result in a degradation of the overall security of the Services during the term of the Agreement.

2. Information Security Management

LogicMonitor shall maintain throughout the term of the Agreement a formal information security management program designed to protect the confidentiality, integrity and availability of Customer Data ("Security Program"). The program shall be documented and updated based on changes in applicable legal and regulatory requirements related to privacy and data security practices.

3. Security Policies and Procedures

LogicMonitor shall maintain formal information security policies and procedures which address the following areas:

A. Risk Assessment & Treatment. Formal risk management processes shall ensure that information security risks are reviewed holistically and have the visibility of executive management.

B. Personnel. Background checks may be conducted for each individual upon hire (except where prohibited by applicable law). Information security training shall be issued within each employee's first week, and annually thereafter.

C. Access Management. Authorization to access business and production systems shall be limited to specific individuals.

D. Change Management. All changes to the Service shall be documented, and each change shall be reviewed, approved, and tested prior to release.

E. Encryption Management. Customer Data shall be encrypted in transit.

F. Vulnerability Management. The Service operating platform shall be scanned for security vulnerabilities on an ongoing, best effort basis, and technical controls shall be maintained to provide a security posture based on defense-in-depth. Upon detection, vulnerabilities will be addressed on a risk prioritized-basis commensurate with that risk.

G. Application Security. The applications which comprise the Service, based on criticality and prioritization may be tested for security defects using multiple testing modalities including static

analysis, dynamic analysis, and software composition analysis where appropriate. Critical and high severity software defects shall be addressed with highest priority.

H. Penetration Testing. Certain aspects of the Service shall be subjected to third-party penetration testing on an annual cadence. Penetration testing shall include, at minimum, the following analyses: information gathering; manual testing of flaws that may compromise the confidentiality, integrity, or availability of Customer Data; escalation of privilege; and system compromise steps.

I. Emergent Threats. For any security vulnerabilities that result in an imminent threat to the confidentiality or integrity of Customer Data, LogicMonitor will use best efforts to address the threat as promptly as possible.

J. Incident Response. LogicMonitor shall maintain a formal incident response procedure to promptly mitigate damages caused by such an incident. Upon confirmation of a security incident that may have impacted the confidentiality or integrity of Customer Data, LogicMonitor shall notify the Customer in writing within 48 hours.

K. Business Continuity Management. LogicMonitor shall maintain a program to ensure ongoing delivery of the Service in the event of a disaster or other significant event that might otherwise impact operation of the business.

4. Data Handling and Protection

LogicMonitor shall maintain formal information security policies and procedures which address the following areas:

A. Service Centers. The Service shall be hosted through geographically distributed data centers operated by third parties, which are memorialized in Exhibit D – The Data Processing Addendum. All data centers shall be certified to AICPA SOC2 Type 2 or equivalent standards, and provide redundant power, cooling, and security systems. LogicMonitor shall review the controls of these facilities at least annually to confirm adequate measures are in place to protect the availability and confidentiality of the Service.

B. Production Servers. All production servers shall be security hardened in accordance with LogicMonitor's policies, have protective software installed, and be monitored for events that impact data security.

C. Data Segregation. LogicMonitor shall maintain no less than industry standard logical data segregation in a multi-tenant environment designed to ensure Customer Data is not accessible by unauthorized individuals. LogicMonitor shall logically isolate Customer Data, and the Customer shall control the specific data stored in the Service. Each customer tenant shall be configured with a unique encryption key to ensure data confidentiality.

D. Data Regionalization. With respect to the Service, Customer may select the service center region in which Customer Data is stored. Customer Data may be transferred to and/or allowed to be accessed by Personnel located in regions in which LogicMonitor provides operations and support services as memorialized in Appendix 3 – Subprocessors, to Exhibit D below. Operational logs and other files submitted for analysis by LogicMonitor's support services shall be stored in the United States. In no event shall any Customer Data or Customer Confidential Information be accessed, stored, or processed from or in any OFAC-sanctioned country.

E. Customer Data Handling. The Service shall maintain appropriate data security controls to address the following areas:

   i. Access controls that may include password strength requirements, multi-factor authentication, single sign-on, and role-based authorization.
   ii. In some cases data access controls including encryption and hashing.
   iii. Audit logging of authentication events.

F. Data Return and Deletion. LogicMonitor will provide a mechanism within the Service to allow for data export, specifically LogicMonitor will provide REST APIs to allow for data to be fetched based on the specified criteria, this may be used to retrieve relevant data upon termination.

5. Business Continuity Management

LogicMonitor shall maintain a formal business continuity management program designed to ensure the continuous operation of business processes which support delivery of the Services. The program shall be documented within LogicMonitor's formal information security policies and procedures, and shall specifically address the following areas:

A. Business Technology Resiliency Planning. All business resources and technology services required for day-to-day business shall be sourced and implemented with resiliency as a primary goal.

   i. LogicMonitor's corporate offices shall be operated such that any office could cease to exist without impact to business operations.
   ii. All LogicMonitor employees shall be issued laptop computers as their personal workstations. In the event a corporate office becomes unavailable for use, employees shall continue to access business systems using internet access provided elsewhere.
   iii. As security controls are implemented and maintained for business technology services, they shall be evaluated to meet continuity requirements.
   iv. Business continuity obligations for the operation of LogicMonitor's Services shall be maintained as defined in Section 5 of this Exhibit.

B. Business Systems Resiliency Testing. LogicMonitor's business continuity plans shall be tested on an ongoing basis. Use of business systems by mobile and remote employees shall be used to provide performance indicators that inform required service levels.

6. Disaster Recovery

LogicMonitor shall maintain a formal disaster recovery program to ensure the resiliency of the Services through multiple types of potentially disruptive events.

A. Architecture for Disaster Recovery. Anticipation of disaster recovery needs shall be a primary consideration in the design and implementation of systems and processes used to operate the Services.

   i. The Services shall operate only out of data centers and IaaS providers that can provide high levels of redundancy in systems that provide power, cooling, network connectivity, fire suppression, flood control, and earthquake resiliency.
   ii. All hardware and network devices shall be deployed with sufficient redundancies to ensure stable and continuous operation that is tolerant of outages that affect both individual components.

iii. Sufficient processes and procedures shall be maintained to meet a Recovery Time Objective (RTO) not to exceed 12 hours. The Recovery Point Objective (RPO) shall not exceed 36 hours. Service Level Indicators shall be maintained to report on overall availability targets.

B. Backup and Restore.

i. All Customer Data stored and processed by the Services shall undergo backup processes to ensure recoverability from incidents which impact security or availability. Backup data shall be created on a frequency targeted to meet the indicated RTO and RPO.

ii. Backup data shall be stored in multiple locations to ensure recoverability from an incident impacting any specific facility. Where backup data is transmitted across public networks, HTTP over TLS shall be used to encrypt transmission.

C. Disaster Recovery Testing.

i. Formal documentation describing the disaster recovery testing process for the Services shall be reviewed and updated at least annually.

ii. The backup/restore procedures upon which the Services' disaster recovery processes are based shall undergo continuous testing as part of regular capacity management exercises.

iii. A complete test of the Services' disaster recovery process, including simulation of datacenter failure, shall be conducted on an annual basis. Each test shall be followed by a report of the testing exercise, confirmation whether current RTO and RPO targets were met, as well as lessons learned and process improvements to decrease RTO and RPO values.

D. Customer Communications. In the case of a significant disruption of the Services, LogicMonitor shall communicate such outages primarily via a notification service located at https://status.logicmonitor.com/. Upon a significant disruption, Customers may also receive notification via email or phone from a technical account manager.

7. Subprocessor Security

LogicMonitor shall conduct security assessments of its subprocessors that process Customer Data to ensure effectiveness of their security operational practices. LogicMonitor's current subprocessors are listed in Exhibit D – Data Processing Addendum.

8. Independent Assessments

On an annual basis, the Security Program shall be audited by an independent third-party to validate compliance with industry standards including the AICPA SOC2 Type 2 trust service principles, ISO/IEC 27001:2013, ISO/IEC 27017:2015, and ISO/IEC 27018:2014. Upon written request, LogicMonitor shall provide evidence of these audit activities in the form of third-party assessment reports and/or certificates. If Customer, in good faith asserts a significant deficiency in any of the third-party assessment reports or certificates mentioned in this section, or if Customer Data is impacted by a security incident, LogicMonitor will respond to the Customer's reasonable written requests for more detailed information relevant to its security and privacy program. LogicMonitor may charge its then-current professional services rates for such responses; however, if it is demonstrated that LogicMonitor is failing to comply with any of its security and privacy obligations under this Agreement, then, LogicMonitor will waive any fees related to the responses and take the necessary steps to remediate the deficiencies at no additional cost to the Customer.

9. Shared Security Model

Notwithstanding the foregoing, Customer acknowledges that security is a shared responsibility between LogicMonitor and the Customer. Customer understands that the Service provides various security controls which must be properly configured according to the "LogicMonitor Security Best Practices" located in the product documentation, to provide adequate protection for Customer Data and infrastructure.

10. Credentials & Authentication

Notwithstanding anything to the contrary, LogicMonitor is not responsible for any harms arising from: (a) Customer's failure to implement and follow password complexity rules and other appropriate digital identity guidelines, which are similar to those found in the NIST 800-63B publication (or similarly rigorous standard); nor (b) Customer's failure to enable (or disabling) two-factor authentication for the Services. If Customer has not enabled, or has disabled two-factor authentication within the Services, Customer must require both proof of possession and proof of control of two different authentication factors in order to authenticate access to the Services for all accounts.

Exhibit B

Service Level Terms

1. **Availability.**

1.1 **Services Availability.** LogicMonitor will use commercially reasonable efforts to ensure that the LogicMonitor Service maintains a Services Availability level of 99.9% for Customer. As used herein, "Services Availability" relates to the core application's availability as served from LogicMonitor hosted environments for data ingestion, alerting, and Customer portal access. Excluding scheduled maintenance periods, the Service will be deemed "available" so long as, (a) data ingestion services are able to accept incoming monitoring data, (b) alerting services are able to generate and attempt delivery of alert messages, and (c) Customer's authorized users are able to login to their Customer portal interface. Services Availability is measured in minutes as a percentage of a particular month (based on a 24-hour day for the number of days in the subject month) that the LogicMonitor Service is available.

1.2 **Scheduled Maintenance.** Services Availability shall not include Planned Maintenance or Extraordinary Circumstances (each as defined in the Terms of Service).

1.3 **Remedies for Services Availability Failure.**

1.3.1 If the Services Availability in the aggregate falls below 99.9% for one (1) calendar month, a Service credit (a "Service Credit") will be available for such month in accordance with the table below. To assess Services Availability, Customer may request the Service Availability for the prior calendar month by filing a LogicMonitor support request ticket through the LogicMonitor support portal. If Services Availability was below 99.9% in the aggregate for the applicable calendar month, Customer may receive the available Service Credit by providing a written request to LogicMonitor for the available Service Credit no later than 60 days after the last day of the calendar month during which the Services Availability failure occurred. Any Service Credit due to the Customer shall be credited to the Customer on the next invoice issued by LogicMonitor under the applicable Service Agreement and if there are no future invoices LogicMonitor will issue payment within 30 days.

Services Availability (Month)	Service Credit
Less than 99.9% but greater than or equal to 99.1%	1% of monthly Service Fees
Less than 99.1% but greater than or equal to 97.5%	5% of monthly Service Fees
Less than 97.5% but greater than or equal to 95%	10% of monthly Service Fees

1.3.2 If (a) the Services Availability falls below 99.9% for any three (3) calendar months in any twelve (12) month period, or (b) the LogicMonitor Service is unavailable for a period of thirty-six (36) consecutive hours, or (c) the Services Availability falls below 95.00% for any one (1) calendar month during any twelve month period, Customer may either (i) immediately terminate the then-current Service Agreement upon five (5) days prior written notice to LogicMonitor and receive a pro-rata refund of pre-paid fees (if any) for periods for which Service has not yet been provided as of the effective date of termination, or (ii) request the Service credits identified in section 1.3.1.

Exhibit C
Technical Support Exhibit

Support Packages

LogicMonitor offers three distinct support tiers—Basic, Enhanced, and Premier—designed to meet the unique needs of our commercial customers. Each tier provides increasing levels of service to ensure your organization gets the right level of support. Additionally, we offer exclusive support for FedRAMP customers, delivering specialized assistance tailored to compliance and security requirements. The table shown here outlines the features included in each package.

SUPPORT PACKAGE		BASIC	ENHANCED	PREMIER	FedRAMP SUPPORT
Self-help resources		✓	✓	✓	✓
Support portal		✓	✓	✓	✓
Account familiarity		⊖	⊖	✓	✓
Initial response times (Inbound tickets)	Urgent (L1)	2 hours	1 hour	1 hour	1 hour
	High (L2)	12 hours	4 hours	4 hours	4 hours
	Normal (L3)	24 hours	8 hours	8 hours	8 hours
	Low (L4)	48 hours	12 hours	12 hours	12 hours
Communication channel	Ticket	✓	✓	✓	✓
	Availability	24x7	24x7	24x7	24x5
	Chat	⊖	✓	✓	✓
	Availability	Not included	24x7	24x7	24x5
	Outbound screen share	⊖	✓	✓	✓
	Availability	Not included	24x7	24x7	24x5
	Inbound phone	⊖	⊖	✓	✓
	Availability	Not included	Not included	24x7	24x7
Support team		Standard	Standard	Premier	FedRAMP
Health Check		⊖	✓	✓	✓
Health Check Remediation Assistance		⊖	⊖	✓	✓
Pro-active support		⊖	⊖	✓	✓

Support Features Descriptions

Account Familiarity

Note: This feature applies only to users with a Premier or FedRAMP support package.
A Customer Success Manager and Premier Support Engineer will schedule an Account Familiarity session with you to capture details about your LogicMonitor account. Information gathered from this session, as well as ongoing support interactions, will be noted in our internal customer knowledge base that help our Premier Support team members develop an understanding of the nuances of your accounts, customizations, or any challenges may have been encountered in the past which can be used to help reduce the resolution time of future support requests.

Identify Named Contacts

Identify your four named contacts, who will be authorized to make inbound phone calls to the Support teams. Named contacts must be LogicMonitor Certified Professionals with administrative access to the account.

Document Account Details

An important part of our Premier account management is to gather information relative to your LogicMonitor environment so that our team becomes more knowledgeable about your account, usage pattern, and other specific configuration settings that will help us provide higher-quality support moving forward. Details to be noted include any custom solutions that have been purchased through Professional Services, integrations in use, critical customizations to the account, collector deployment caveats, and other pertinent information Support should be made cognizant of.

Open Case Reviews

A review of any open or long-standing issues impacting Premier customers will be conducted. Any existing open support cases opened with Standard Support team will be transferred over to Premier Support Engineers for on-going ownership and resolution.

Review Support Channels and Processes

A review of current processes for contacting support relevant to Premier Support customers including: Chat Channel, Inbound Phone Calls, Ticket Portal, Escalations, scheduling, and after-hours availability.

Located Support Channels

Note: This feature applies only to users with a Premier or FedRAMP support package.
You have dedicated communication channels that route your requests directly to the Premier Support team 24×5. To maintain 24×7 availability, Premier Support requests made outside of the hours of Premier Support team availability will be routed to the Standard Support channels at a higher priority for assistance. If the request is urgent in nature, the Standard Support team will be capable of escalating Premier Support requests to the On-Call Premier Support Engineer.

Note: If specific coverage is required outside of the regular hours of availability, time can be scheduled in advance with Premier Support engineers for specific tasks best reserved outside the normal business hours or work week. This is subject to scheduling and availability and requires at least 1 weeks notice for confirmation.

Health Check

Health Checks are an assessment of your account to provide actionable recommendations for improving LogicMonitor configuration and feature usage. Health checks are a great preventive tool for identifying misconfigurations or inefficiencies within your account that could lead to potential interruptions or missed notifications.

Health Checks typically cover the following focus areas:

- Alert settings

- Alert volume
- Collectors
- Dashboards
- Devices
- Integrations
- LogicModules
- Reports
- User access
- Website

Health Check Remediation Assistance

Note: This feature applies only to users with a Premier or FedRAMP support package.
You have the option to get Remediation Assistance on recommendations identified during the Health Check assessment. Premier and FedRAMP Support customers may schedule up to (three) 2-hour working sessions/ per quarter with a Premier Support Engineer who can advise on best practices and aid with remediation on flagged focus areas.

Pro-Active Support

Note: This feature applies only to users with a Premier or FedRAMP support package.
For our Premier and FedRAMP customers we offer the option to Opt-In to Pro-active Support, in which your accounts are monitored for significant changes and other activity that might be beneficial for administrators to be aware of. LogicMonitor Premier Support Engineers will do regular checks on a set of predefined items for your accounts. If any concerns are identified, a support ticket will be opened on your behalf to highlight the concern with options to assist with resolving.

Examples of items to be monitored include, but are not limited to:

- Spikes in alert activity across the account
- Increased number of dead collectors within the account
- Significant variances in the number of resources within the account
- Outdated Core LogicModules in use
- No Data being collected on critical devices
- Checks for Known Bugs impacting customer accounts

Communication Channels
LogicMonitor supports several channels for communication between customers and support engineers.

Chat

Chat is the primary communication channel for customers on a paid Support package from the LogicMonitor Support Portal located at https://support.logicmonitor.com. LogicMonitor has recognized online chat to be the most effective channel for troubleshooting customer issues; allowing LogicMonitor Technical Support Engineers (TSEs) to work real time with our customers while being able to share artifacts that make the troubleshooting process more efficient. Artifacts such as screenshots, log files, code snippets, etc., can all be uploaded and shared real time within the chat interface; resulting in a faster resolution. Requests for support via chat are handled on a first-come-first-serve basis.

Support Ticket

Support tickets can be created by customers on all Support packages from the LogicMonitor Support Portal located at https://support.logicmonitor.com. In the event of a Service Disruption, in which customers cannot access their account, support tickets can still be submitted through the Support Portal. Urgent priority tickets are managed at the highest priority over any other communication channel (chat, phone, other ticket priorities), and should be reserved for items that are severely impacting customers' accounts. To help us resolve requests in a timely manner, customers should provide as many details as possible about their request, including specific examples of target areas to investigate or attaching any relevant screenshots and log files.

Screen Share (Outbound)

LogicMonitor Support utilizes screen shares to work with our customers on requests that are sometimes best handled outside of text format or need a more guided approach. Customers on a Paid Support package may request an outbound screen share with a LogicMonitor Technical Support Engineers (TSEs) once they have reached out to coordinate via one of our other communication channels (Chat or Support Ticket) and have provided a summary of the issue.

Phone call (Inbound)

Inbound phone calls to Support are available only to customers on a Premier or FedRAMP support package. Premier and FedRAMP Support customers will receive a phone number to contact LogicMonitor Support, which can be used by authorized named contacts identified during the Account Familiarity process.

Status Page

LogicMonitor maintains an external Systems Status Page to keep customers informed of service disruptions. It is highly recommended that our customers subscribe to our status page so that they are notified as soon as possible when LogicMonitor is experiencing technical difficulties. Initial updates are posted as soon as issues are identified and updates will be provided throughout the Service Disruption until resolution.

Issue Severity Levels

LogicMonitor is committed to provide outstanding, responsive Support and will make reasonable efforts to meet the target initial response time for the applicable severity or priority levels. Initial responses provided will be meaningful and related to the inbound support request. Response times are for initial response and

acknowledgment of inbound requests; they are not meant to imply time to resolve the request. As highlighted in the following table, issues are assigned one of four severity levels.

Severity	Description	Examples	Customer Success Engagement and Escalation
Urgent (L1)	Usage of LogicMonitor is severely impacted to the degree that the product is unusable.	● Portal is unreachable ● Portal performance is degraded to a degree severely impacting overall usability ● Multiple alerts generated where data does not indicate a breach of configured thresholds, or valid alerts failed to generate in-portal ● Total loss of monitoring, data ingestion, or processing for resources, LM Logs, or Websites ● Multiple “Collector Down” alerts simultaneously	Support team will engage the Customer Success team in under four hours if a solution is not found. Customer Success team will follow the documentation and communication policy procedures for Urgent case handling-notifying management.
High (L2)	Issues with the product that are causing previous working conditions to fail, or that degrade the ability for LogicMonitor to perform primary Observability functions. Issues affecting multiple resources.	● Any alert generated where data does not indicate breach of set thresholds, or a valid alert failed to generate in-portal ● Issues affecting documented API endpoints Loss of monitoring or data ingestion for a subset of resources, LM Logs, or websites ● Loss of historical data Collector performance issues impacting multiple collectors ● Issues causing a limited performance impact within the LM portal or affecting resources, LM Logs, or Websites within the portal	Support team will engage the Customer Success team within 48 hours if a solution is not found. Customer Success team will work with Support teams, including Support Managers to facilitate communication and resolution.

		Collected data fails to plot to graphs and widgets ● Total failure of any individual LogicMonitor feature	
Normal (L3)	Issues regarding product configuration or with establishing new monitoring for Resources, LM Logs, or Websites. Issues affecting a single resource. Performance degradation in functionalities secondary to Observability.	● Issues affecting a single resource, website, collector, dashboard or widget, report, or LM Logs ● Alert generates in portal but notification fails to route properly ● Issues applying to monitoring or adding new resources ● Issues causing a minimal impact to usability of the LogicMonitor Portal but not impacting Monitoring or Alerting	Support team will engage the Customer Success team as needed.
Low (L4)	Questions of a more general nature or issues not directly impacting product usage.	● General questions regarding monitoring availability or product functionality ● Requests for new features ● Requests for best-effort assistance with graph, report, or expression tuning Mobile app issues ● Other issues not impacting product usability	Support team will engage the Customer Success team as needed.

Important: Severity levels (and their associated response times and escalation procedures) do not apply to feature or UX requests, LogicModule creation requests, misconfiguration errors, bugs not impacting performance/functionality, product training, or Professional Services engagements.

Premier Support Team Availability

Note: This feature applies only to users with the Premier support package.

You will have direct access to the Premier Support team 24×5, excluding LogicMonitor company holidays per region. Outside these hours of availability, when the Premier Support team is not available, Premier Support customer requests are handled by the Standard support team. 24×5 coverage begins every Sunday at 07:00PM CST and closes every Friday at 06:59PM CST (Monday 12:00AM to Friday 11:59PM UTC).

FedRAMP Support Availability and Coverage

The FedRAMP Support tier provides dedicated assistance for government and regulated customers. Inbound phone support is available 24×7, ensuring continuous access to technical expertise when it's needed most. Ticketing, chat, and outbound screen sharing are available 24 hours a day, Monday through Friday, to support operational needs. While initial coverage is limited, future enhancements will further expand support availability.

US Holidays	EMEA Holidays	APAC Holidays
New Year's Day	New Year's Day	New Year's Day
Martin Luther King Jr. Day	Good Friday	Chinese New Year
President's Day	Easter Monday	Good Friday
Memorial Day	May Bank Holiday	Labour Day
Juneteenth	Spring Bank Holiday	Hari Raya Puasa
Independence Day	Juneteenth	Vesak Day
Labor Day	Summer Bank Holiday	Juneteenth
Veteran's Day	Christmas Day	Hari Raya Haji
Thanksgiving Day	Boxing Day	National Day
Day After Thanksgiving		Deepavali
Christmas Day		Christmas Day
Christmas Eve		

Limitations of Support. **Support does not include the following:**

- Development of custom scripts, LogicModules, or integrations with third-party applications.
- Inbound Phone Support for customers not on a Premier Support package and users other than the designated contacts identified during Account Familiarity processing.
- Support for custom solutions developed by the customer or delivered by LogicMonitor Professional Services and its partners.
- Support, analysis of, or troubleshooting third-party vendor add-ons or products.
- Collectors that are installed on operating systems that are end of life. LogicMonitor follows the Microsoft Lifecycle Policy (“Extended Support End Date”) and the Red Hat Enterprise Linux Life Cycle (“End of Maintenance Support 2 (Product retirement date) when determining which Windows and Linux server operating systems are supported for Collector installation. For more information, see Installing Collectors.
- Feature requests, product improvements, or additional commitments from the product or development teams.
- Non-English language support.
- Providing remote administration or taking control of a customer’s environment to perform installations, configurations, or adjustments to resources outside of the LogicMonitor platform.
- On-site support at the customer location.

Exhibit D

LOGICMONITOR DATA PROCESSING ADDENDUM (DPA)

Applies To: Customer subscription(s), or partner agreements referencing this DPA.
Scope: Global, applicable privacy laws such as CCPA and CPRA, PIPEDA, UK GDPR, Swiss Data Privacy Laws, and the GDPR.

This Data Processing Addendum (this **"Addendum"** or **"DPA"**) supplements and will have the same effective date as the Service Agreement (the **"Agreement"**) entered into by and between the applicable LogicMonitor entity (**"LogicMonitor"**) and the **Customer** named in the LogicMonitor Order Form (**"Customer"**), date of acceptance of product terms of service, or the applicable Agreement referencing this DPA (each may be referred to as a **"party"** and collectively the **"parties"**).

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. Introduction: Services and Background

1.1. **IT Systems Performance Monitoring.** The parties understand that the purpose and focus of the SaaS Service is IT systems status and performance monitoring and not to function as a receptacle, conduit or service to store, manipulate, transmit, retrieve or process Personal Data.

1.2. **Low Volume of Personal Data.** Nonetheless, the parties acknowledge that the incidental capturing of nominal Personal Data (as defined herein) in connection with the Service will occur in the ordinary course (for example, credentials (login) information for authorized users and information in log files with transactional monitoring, and names and contact information of employees of each party as needed to conduct the SaaS Services and business relationship).

1.3. **Purpose.** The purpose of this Addendum is to provide that the parties shall manage their operations and activities with respect to Personal Data in a confidential and secure manner and in accordance with all applicable laws and regulations.

2. Definitions

2.1. "**Affiliate(s)**" has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term means any entity that directly or indirectly controls, is controlled by, or is under common control or ownership with a party, where "control," "controlled by" and "under common control with" means the possession of the power to direct, cause or significantly influence the direction of the entity, whether through the ownership of voting securities, by contract, or otherwise;

2.2. "**California Data Protection Laws**" means the California Consumer Privacy Act of 2018 (or **"CCPA"**), as amended by the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq. (or **"CPRA"**), and all regulations issued pursuant to it;

2.3. "**Contracted Processor**" means LogicMonitor or LogicMonitor Affiliate and/or a Sub-processor, as the context requires;

2.4. “**Controller to Processor SCCs**" and **“Controller to Controller SCCs”** reference Module 2 and Module 1 (respectively), and Module 3 (if both parties are considered “Processors”) of the EU Standard Contractual Clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as described and is available here; as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws;

2.5. "**Data Protection Laws**" and “**Applicable Law**” means the California Data Protection Laws, EU Data Protection Legislation, Swiss Data Protection Law, UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

2.6. “**Data Subject**” (whether or not capitalized) means an identified or identifiable natural person as defined in the GDPR;

2.7. "**Data Controller**" or **“Controller”** means the entity which determines the purposes and means of Processing Personal Data (in this case, Customer) as defined in the GDPR, and shall include a “business” as that term is defined in the California Data Protection Laws;

2.8. "**Data Processor**" or **“Processor” means** the entity which Processes Personal Data on behalf of the Data Controller (in this case, LogicMonitor) as defined in the GDPR, and shall include a “service provider” as that term is defined in the California Data Protection Laws**;**

2.9. "**EEA**" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein;

2.10. "**EU Data Protection Legislation**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the Processing of personal data and on the free movement of such data, including any applicable national implementations thereof, (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**"), including any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR, and (iii) any guidance or codes of practice issued by a governmental or regulatory body or authority in relation to compliance with the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time;

2.11. "**Restricted Transfer**" means a transfer of Personal Data by Customer or any Customer Affiliate to LogicMonitor or any LogicMonitor Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by Data Protection Laws in the absence of the protection for the transferred Personal Data provided by an adequate transfer mechanism such as the Controller-to-Processor SCCs, or the UK IDTA (defined below);

2.12. "**Member State**" means a member state of the EU;

2.13. "**Personal Data**" means any data, information or record that directly or indirectly identifies a natural person (Data Subject) or relates to an identifiable natural person, including but not limited to, name, address, telephone number, email address, payment card data, identification number such as social security or tax ID number, date of birth, driver's license number, medical and health-related information, and any other personally identifiable information that LogicMonitor or any third party acting on LogicMonitor's behalf Processes in connection with this Agreement, and includes "personal data" as is defined in the GDPR and "personal information" as is defined in the California Data Protection Laws;

2.14. "**Process**," "**Processes**," "**Processing**" or "**Processed**" means any operation or set of operations which is performed on any data, information, material, work, expression or other content, whether or not by automated means, such as collection, recording, downloading, uploading, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

2.15. **"Sale,"** or **"Sell,"** or **"Share"** have the meanings assigned to them in the California Data Protection Laws, or as otherwise defined under Applicable Law;

2.16. **"Security Incident"** means any suspected or actual loss, unauthorized or unlawful Processing, destruction, damage, or alteration, or unauthorized disclosure of, or access to the Personal Data;

2.17. **"Service Provider"** has the meaning assigned to it in the California Data Protection Laws;

2.18. **"Sub-processor"** means any party engaged by LogicMonitor in order to Process Personal Data in the course of providing services to Customer;

2.19. "**Supervisory Authority**" means (a) an independent public authority which is established by an EU Member State pursuant to EU Data Protection Legislation, and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

2.20. "**Swiss Data Protection Law**" means the Swiss Federal Act on Data Protection;

2.21. "**Swiss Restricted Transfer**" means a transfer of Personal Data by Customer or any Customer Affiliate to LogicMonitor (or any onward transfer), in each case, where such transfer would be prohibited by Swiss Data Protection Law in the absence of the protection for the transferred Personal Data provided by the Controller to Processor SCCs or Controller to Controller SCCs, the UK IDTA or similar transfer mechanism, subject to Switzerland-specific modifications as set out in this DPA;

2.22. "**UK Data Protection Laws**" or simply **"UK GDPR"** means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and other data protection or privacy legislation in force from time to time in the United Kingdom;

2.23. "**UK IDTA**" means, the **International Data Transfer Addendum** to the EU Commission Standard Contractual Clauses (or successor mechanism), effective March 21, 2022; which is available here, and may be amended or replaced from time to time, pursuant to Article 46 of the UK GDPR.

3. General Applicability

3.1. **Generally.** This Addendum shall apply to the extent LogicMonitor Processes Personal Data, in the course of performing services, of Data Subjects on behalf of Customer or a Customer Affiliate.

3.2. **Terms for Resellers and Other Partners.** Notwithstanding the foregoing, as between LogicMonitor and any entity acting solely as a reseller, distributor, or other partner (meaning a party who is not directly using the LogicMonitor services for its own business use) (each a **"Partner"**), the parties agree that the scope of this DPA is limited to the terms applicable to independent Controller relationships only, including those terms in **Section 6 – Terms for Partners**.

4. Processing of Personal Data

4.1. **Purpose Limitation.** LogicMonitor will only Process the types of Personal Data, and only in respect of the categories of Data Subjects, and only for the nature and purposes of Processing and duration, as is set out in Appendix 1, and on behalf of and in accordance with Customer's written instructions.

4.2. **Business Purpose.** LogicMonitor shall only Process Personal Data for **"business purposes,"** as such term is defined under the California Data Protection Laws, including: (i) providing the Services to Customer; (ii) helping to ensure the security and integrity of Personal Data; (iii) debugging to identify and repair errors that impair existing intended functionality; and (iv) undertaking activities to verify or maintain the quality or safety of the Services.

4.3. **No Sale or Sharing of Personal Data.** LogicMonitor is prohibited from Selling or Sharing Personal Data, as such terms are defined under the California Data Protection Laws.

5. Roles and Responsibilities

5.1. **Responsibilities and Appointment.** Customer (as Controller, or Processor as the case may be) appoints LogicMonitor as a Processor to Process the Personal Data on Customer's behalf. However, where Customer may be a Processor, it appoints LogicMonitor as Customer's Sub-processor.

5.2. **Compliance.**

5.2.1. LogicMonitor, as Processor, or Sub-processor, will comply with all applicable Data Protection Laws.

5.2.2. To the extent that Customer is deemed a Controller under Applicable Law, Customer, as Controller, shall: (i) comply with all applicable Data Protection Laws; (ii) ensure that any instructions that it issues to LogicMonitor shall comply with Data Protection Laws; (iii) have sole responsibility for the accuracy, quality and legality of the Personal Data provided to LogicMonitor; (iv) have established the legal basis for Processing under Data Protection Laws; (v) have provided all notices and obtained all consents as may be required under Data Protection Laws and (vi) ensure that it has and will continue to have, the right to provide access to the Personal Data to LogicMonitor in accordance with the terms of the Agreement and this Addendum.

5.2.3. If LogicMonitor believes that any instruction from Customer is in violation of, or would result in Processing in violation of Applicable Law, then LogicMonitor will promptly notify Customer, and if Customer believes LogicMonitor is or may be in violation of Applicable Law it will promptly notify LogicMonitor. Similarly, if Applicable Law requires LogicMonitor (or, for avoidance of

doubt, any Sub-processor) to conduct Processing that is or LogicMonitor believes could reasonably be construed as inconsistent with Customer's instructions, LogicMonitor will notify Customer promptly prior to commencing the Processing, unless this notification is prohibited by law on important grounds of public interest.

5.2.4. If LogicMonitor determines it can no longer meet its obligations under Applicable Law, it must promptly notify Customer and suspend all Processing of Personal Data until appropriate remedial actions are taken.

5.2.5. Each party shall maintain records of all Processing operations under its responsibility that contain at least the minimum information required by Data Protection Laws, and shall make such information available to any Supervisory Authority on request.

6. Terms for Partners

6.1. **Applicability.** This section does not apply to the LogicMonitor subscription services to Customers. This section only applies to Partners. LogicMonitor and Partner agree that the sharing of some Personal Data may be required to fulfill each party's respective obligations under the applicable agreement (such as a reseller arrangement) and have therefore agreed to these **Terms for Partners**.

6.2. **Partners Comply with Applicable Law.** Partner and LogicMonitor agree that each party shall independently comply with their respective obligations under Data Protection Laws, including: (i) Processing shared Personal Data in accordance with the principles of lawfulness, fairness, and transparency, and respect the rights of Data Subjects; and (ii) facilitating the rights of Data Subjects including access, rectification, erasure, and data portability; and (iii) in the event of a Security Incident, the affected Party shall notify the other Party without undue delay and cooperate with the requirements of the relevant Data Protection Laws.

6.3. **International Data Transfer and Compliance:** The Parties will conduct all Restricted Transfers in accordance with the legal requirements of the jurisdictions involved, including but not limited to executing SCCs where necessary in other arrangements, ensuring adequate level of data protection in the recipient country, and complying with local laws in non-EU jurisdictions such as Japan, India, and Singapore. The Parties agree to abide by the Controller to Controller SCCs (or similarly restrictive transfer mechanism, to the extent applicable) when engaging in any Restricted Transfer or cross-border transfer of Personal Data to any jurisdiction without an adequacy decision.

6.4. **Data Sharing Principles:** The Parties commit to the following principles whenever sharing Personal Data: (i) Personal Data shall be collected and Processed only for mutually agreed purposes (purpose limitation); and (ii) only necessary Personal Data for the agreed purposes are shared and Processed (data minimization); and (iii) regular updates and improvements will be made to maintain data accuracy and employing appropriate security measures designed to protect Personal Data integrity (protection of data integrity); and (iv) each party will adhere to agreed-upon retention periods designed to ensure safe disposal or return of Personal Data upon termination of this DPA or applicable Partner agreement.

7. Confidentiality and Security

7.1 **Security Program**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, LogicMonitor will maintain or cause to be maintained a reasonable and commercially feasible information security program that complies with all Applicable Laws and is designed to reasonably ensure the security and confidentiality of all Personal Data.

7.2 **Security Measures**. LogicMonitor will take all appropriate and commercially reasonable measures, including, without limitation, administrative, physical, technical (including electronic), and procedural safeguards designed to protect Personal Data against the risks of a Security Incident (the **"Technical and Organizational Measures"**). This includes maintaining a business continuity and disaster recovery plan (BCP/DR), a written information security program (WISP), as well as the Technical and Organizational Measures described in Appendix 2, which is hereby incorporated by reference. LogicMonitor will take commercially reasonable measures to ensure that Personal Data is only available to LogicMonitor personnel and its agents and Affiliates who have a legitimate business need to access Personal Data, who are bound by legally enforceable confidentiality obligations, who have received training on applicable data protection policies and procedures, and who will only Process the Personal Data in line with Customer's instructions.

7.3 **Confidentiality of Processing**. LogicMonitor shall ensure that any person that it authorizes to Process Personal Data (including its staff, agents, subcontractors and Sub-processors) shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

7.4 **Security Incident Response and Notification**.

7.4.1 With respect to any Security Incident regarding Personal Data of which LogicMonitor becomes aware, in addition to its obligations set forth in other sections of this DPA, LogicMonitor will promptly and without undue delay, notify Customer and provide such timely information as Customer may reasonably require to enable Customer to fulfill any data breach reporting obligations under Data Protection Laws. The notice will summarize in reasonable detail the nature of the Security Incident; whether the suspected data is lost, stolen or compromised, if known; LogicMonitor's appraisal of the consequences of the Security Incident; the corrective action taken or to be taken by LogicMonitor; and any internal point(s) of contact responsible for managing or responding to the Incident, including the contact information LogicMonitor's Data Protection Officer (**"DPO"**). LogicMonitor will promptly take all reasonably necessary and advisable corrective actions and will cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate, or rectify such Security Incident.

7.4.2 In the event of a Security Incident, if either party determines that any Security Incident must be disclosed or reported to a third party, including individuals or governmental authorities (including any Supervisory Authority), each party will fully cooperate with and assist the other party in fulfilling such reporting and disclosure obligations. Unless required by Applicable Law, LogicMonitor shall not make any notifications to a Supervisory Authority or any Data Subjects about the Security Incident without the Customer's prior written consent (not to be unreasonably withheld or delayed).

8. Sub-processors

8.1 **Appointment of Sub-processors**. Customer agrees that LogicMonitor may engage LogicMonitor Affiliates and third-party Sub-processors to Process the Personal Data on LogicMonitor's behalf on the basis of general authorization, and as otherwise restricted by this DPA.

8.2 **Sub-processor Requirements.** Whenever LogicMonitor engages the services of Sub-processors, LogicMonitor agrees that such Sub-processors are capable of maintaining appropriate safeguards for Customer's Personal Data and that LogicMonitor has contractually obligated such Sub-processors to maintain appropriate safeguards designed to comply with Applicable Law and to protect the Personal Data to the same standard provided for by this DPA.

8.3 **Sub-processor List and Objections.** A list of current Sub-processors is maintained in LogicMonitor's **Data Handling Supplement**, available at available at https://www.logicmonitor.com/data-handling-supplement (which location may be updated by LogicMonitor from time-to-time and Customer will be notified of such new location) (the **"Listing"**). If LogicMonitor engages a new Sub-processor (**"New Sub-processor"**), LogicMonitor shall update the Listing and send a notification by email to Customer at its primary business e-mail contact, or to any privacy contact(s) designed by Customer through the Service portal. Customer may object to the engagement of such New Sub-processor by notifying LogicMonitor within ten (10) days of LogicMonitor's notification, provided that such objection must be on reasonable, substantial grounds, directly related to such New Sub-processor's ability to comply with substantially similar obligations to those set out in this Addendum (an **"Objection"**). LogicMonitor shall have the right to cure any Objection, provided, that if it determines the same is not curable, it will notify Customer and if the parties are not able to reach a reasonable resolution, either party may terminate the Agreement upon thirty (30) days' notice. If the Customer does not so object, the engagement of the New Sub-processor shall be deemed accepted by the Customer.

8.4 **Liability**. LogicMonitor will be liable for the acts and omissions of its Sub-processors to the same extent that LogicMonitor would be liable if performing the services of each Sub-processor directly. Upon request, LogicMonitor will make available to Customer a current list of Sub-processors that Process Personal Data in connection with this Agreement.

9. Government Access Requests

9.1 **Notice of Access Requests.** LogicMonitor will promptly notify Customer of any request for access to any Personal Data from any regulatory body, government official or other third person.

9.2 **Responding to Access Requests.** LogicMonitor will cooperate with Customer if Customer, its regulators or a data subject requests access to Personal Data for any reason, provided that the Customer shall be responsible for LogicMonitor's reasonable costs and expenses arising from such cooperation.

9.3 **Transfer Impact Assessment.** Where required by Data Protection Legislation, LogicMonitor will maintain a **"Transfer Impact Assessment"** covering the transfer of Personal Data, pursuant to the provision of services, from an EU country to the United States. LogicMonitor will provide such upon request by Customer.

10. Retention and Destruction of Personal Data

10.1. **Deletion and Return of Personal Data.** Except for Retained Data required by law (defined below), LogicMonitor will not retain Personal Data any longer than is reasonably necessary to accomplish the intended purposes for which the data was Processed pursuant to this Agreement, and except as required under Applicable Law or in order to defend any actual or possible legal claims as the Customer so directs, LogicMonitor shall take reasonable steps to return or irretrievably delete all Personal Data in its control or possession when it no longer requires such Personal Data to exercise or perform its rights or obligations under this Agreement, and in any event on expiry or termination of this Agreement.

10.2 **Legal Purposes and Retained Data.** To the extent that LogicMonitor is required by Applicable Law to retain all or part of the Personal Data (the "**Retained Data**"), LogicMonitor shall: (i) cease all Processing of the Retained Data other than as required by the Applicable Law; and (ii) keep confidential all such Retained Data in accordance with the applicable confidentiality and security

requirements of the applicable agreement and this DPA; and (iii) continue to comply with the provisions of this DPA in respect of such Retained Data.

11. Security Reports and Audit

11.1 **Audits**. To the extent that LogicMonitor is engaged in Processing Personal Data for Customer under the Agreement, Customer will have the right to verify compliance by LogicMonitor and any Sub-processor with the terms of this Agreement or to appoint a third party under reasonable covenants of confidentiality acceptable to the parties to verify the same on Customer's behalf. LogicMonitor will grant Customer or its agents' access, at mutually acceptable times, and no more than once annually, to the extent necessary to accomplish the inspection and review of the procedures relevant to the protection and Processing of Personal Data. LogicMonitor and Customer will consult and agree on the reasonable start date, scope and duration and security and applicable confidentiality controls for the audit. LogicMonitor agrees to provide reasonable assistance to Customer in facilitating this inspection function. Customer shall provide LogicMonitor with any audit reports generated in connection with any audit at no charge unless prohibited by Applicable Law, the audit reports shall be confidential, and Customer may use the audit reports only for the purposes of meeting its audit requirements under Applicable Law and confirming compliance with the requirements of this Addendum. Nothing in this Section shall require LogicMonitor to breach any duties of confidentiality owed to any of its clients, employees or third-party providers, and all audits shall be at Customer's sole cost and expense.

11.2 **Security Reports**. Any provision of security attestation or audit reports (such as SOC 2, Type II or equivalent) shall take place in accordance with Customer's rights under the Agreement. If the Agreement does not include a provision regarding security attestation reports or audit rights, LogicMonitor shall provide a copy of its most current security report upon Customer's written request and subject to the confidentiality provisions of the Agreement. Such reports are generally available on the LogicMonitor Trust Center (available at: trust.logicmonitor.com).

11.3 **Privacy Impact Assessments.** To the extent required by Data Protection Laws, LogicMonitor will cooperate and assist Customer with a privacy impact assessment or data protection impact assessment (or similarly named assessment), by providing information (to the extent not already provided to Customer) and cooperation as reasonably necessary.

12. Rights of Data Subjects

12.1. **Data Subject Rights Generally.** LogicMonitor will assist Customer as requested with responding to Data Subjects' requests to exercise their rights under Applicable Law and regulations, which may include, without limitation, rights of access, correction, amendment, blocking and deletion. LogicMonitor will notify Customer promptly if it receives any such request or claim from a Data Subject relating to Personal Data or LogicMonitor's Processing thereof. For the avoidance of doubt, Customer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure or data portability involving that Data Subject's Personal Data.

13. Restricted Transfers

13.1 **Generally.** In respect of any Restricted Transfer, Customer and each Customer Affiliate (each as **"Data Exporter"**) and LogicMonitor and each LogicMonitor Affiliate (each as **"Data Importer"**) with effect from the commencement of the relevant transfer hereby enter into the Controller to Processor SCCs. The parties agree that: (i) Annex 1 to the Controller to Processor SCCs shall be deemed to be pre-populated with the relevant sections of Appendix 1 - Description of the Processing, below; and (ii) the Processing operations are deemed to be those described in the

Agreement; and (iii) Annex 2 to the Controller to Processor SCCs shall be deemed to be pre-populated with the relevant sections of Appendix 2 - Technical and Organizational Measures; and (iv) Annex 3 to the Controller to Processor SCCs shall be deemed to be pre-populated with the language in Appendix 3 - Sub-processors. All appendices are incorporated by reference into this DPA.

13.2 **Restricted Transfers - Switzerland**. In respect of any Swiss Restricted Transfer, Customer and each Customer Affiliate (each as **"Data Exporter"**) and LogicMonitor and each LogicMonitor Affiliate (each as **"Data Importer"**) with effect from the commencement of the relevant transfer hereby enter into the Controller to Processor SCCs to be completed, subject to the following modifications:

i. For purposes of Annex I.C and Clause 13 of the Controller to Processor SCCs, insofar as the data transfer is governed by the Swiss Data Protection Law, the Supervisory Authority shall be Switzerland's Federal Data Protection and Information Commissioner (FDPIC);

ii. The term **"Member State"** must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in Switzerland in accordance with Clause 18(c) of the Controller to Processor SCCs.

iii. The Controller to Processor SCCs shall protect the data of Switzerland legal entities until the entry into force of the 25 September 2020 revised version of the Swiss Federal Act on Data Protection.

iv. Any reference in the Controller to Processor SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss Data Protection Law.

13.3 **Restricted Transfers – United Kingdom.** In respect of any Restricted Transfer subject to UK Data Protection Laws, Customer acting on its own behalf and as agent for each Customer Affiliate (each as **"Data Exporter"**) and LogicMonitor acting on its own behalf and as agent for each Contracted Processor (each as **"Data Importer"**) with effect from the commencement of the relevant transfer hereby enter into the UK IDTA.

13.3.1 **UK IDTA:** The parties agree that the UK IDTA will be deemed to be pre-populated with the relevant provisions of Appendix 1 - Description of the Processing, Appendix 2 - Technical and Organizational Measures, and Appendix 3 - Sub-processors.

13.4 **Effective Date for SCCs.** The Controller to Processor SCCs, and the UK IDTA made under this DPA, as applicable, come into effect on the later of: (i) the Data Exporter becoming a Party to this Agreement; or (ii) the Data Importer becoming a Party to this Agreement; or (iii) the commencement of the Restricted Transfer to which the Controller to Processor SCCs, or the UK IDTA relate.

13.5 **Updates to Transfer Requirements.** If, at any time, a Supervisory Authority or a court with competent jurisdiction over a Party mandates that transfers from Controllers in the EEA or the UK to Processors established outside the EEA or the UK must be subject to specific additional safeguards (including but not limited to specific technical and organizational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Personal Data is conducted with the benefit of such additional safeguards.

14. Miscellaneous

14.1 **Order of Precedence**. This DPA supersedes any other provision of the Agreement to the extent such provision relates to the privacy, confidentiality or security of Personal Data; provided, however, in the event of any conflict between the provisions of this DPA and the other portions of the Agreement, the parties will comply with the obligations that provide the most protection for Personal Data. Except as amended by this DPA, the Agreement will remain in full force and effect.

If there is a conflict between the Agreement and this DPA, the terms of this DPA will control. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to the exclusions and limitations set forth in the Agreement.

14.2 **Limitation of Liability.** The total liability of each Customer and LogicMonitor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement, except to the extent that such limitation is invalid under Applicable Law.

14.3 **Governing Law.** This DPA will be governed by and construed in accordance with the law stated in the Agreement, except to the extent that applicable Data Protection Laws require otherwise, in which event this DPA will be governed in accordance with applicable Data Protection Laws and, if applicable, be subject to the jurisdiction of the relevant Data Exporter that exported the Personal Data from the EEA.

APPENDIX 1 – DESCRIPTION OF THE PROCESSING

1. **Exporter Details.**

Data Exporter: Customer's name as listed on the applicable Agreement or order form.

Address: The address associated with Customer's applicable order form, or invoice, or as otherwise agreed.

Contact details: The contact details for Customer are as listed on the applicable Agreement or order form.

Role: Controller (unless otherwise indicated in the applicable order form).

2. **Importer Details.**

Data Importer: LogicMonitor, Inc. (or the LogicMonitor entity listed in the Agreement).

Address: 820 State Street, 5th Floor, Santa Barbara, CA 93101

Contact details: Timothy Tesch, DPO, privacy@logicmonitor.com

Role: Processor (unless otherwise indicated in the applicable order form).
Activities relevant to the data transferred under these Clauses: LogicMonitor primarily Processes IT systems health, status and performance data from Customer's information technology systems. Incidental Personal Data elements Processed may include name, email address, mobile device number, and workstation IP address, upon the instruction of the Customer.

3. **Processing Details.**

Subject matter of processing: The subject matter of the Processing is the performance of services, as described in the applicable Agreement.

Frequency and duration of the processing: For the duration of the Agreement.

Nature and purpose of the processing or transfer: LogicMonitor may Process Personal Data within normal operation of the service, typically for automated procedures such as notification delivery (email/SMS), audit logging and user support.

Categories of Personal Data: Access (login) credentials, email addresses, mobile device numbers, workstation IP addresses.

Categories of Data Subjects: Employees, temporary workers and contractors assigned by Customer to use the SaaS Services.

Competent Supervisory Authority: Applicable Supervisory Authority of the EU Member State in which Customer Primarily Resides.

APPENDIX 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

1. **Entry control.** Unauthorized persons are prevented from entering data processing facilities where Personal Data is processed and used.
   a. **Measures:** LogicMonitor's service platform is operated as a hybrid deployment across co-located data centers and AWS resources. Both LogicMonitor's data center subservice provider and AWS maintain stringent controls around the physical and environmental security of each site. In our data center facilities a five-step process is required to gain physical access to LogicMonitor servers, including a 24x7x365 manned security check, electronic keycards, and successive biometric scanning at each point of access. High-resolution video surveillance is maintained throughout the facilities.

2. **Data processing systems access control.** Unauthorized persons are prevented from using data processing systems (**"DP Systems"**).
   a. **Measures**: Access to the networks that contain customer data require authentication via a centrally-managed Single Sign-On (**"SSO"**) service. LogicMonitor's SSO system enforces the use of strong password policies, including password expiration, restrictions on password reuse, and minimum password strength. Two-factor authentication is enforced to further protect against unauthorized access. Following successful authentication and authorization based on role, tertiary authentication against a privileged access management system is required to access any systems containing customer data.

3. **Data access control.** Measures are to be taken to ensure that only persons authorized to use a DP System may only access the data for which they have been granted access, and, while Processing and using Personal Data and after it has been saved, it is not possible for such data to be read, copied, edited or deleted.
   a. **Measures**: The LogicMonitor service has been designed with sophisticated role-based authorization features that allow our customers to limit access to any type of collected data based on the principle of least privilege. LogicMonitor provides a number of default roles out-of-the-box, but the customer is solely responsible for the access rights assigned to each role and the assignment of roles to individuals.

4. **Data transfer control.** Measures are to be taken to ensure that Personal Data cannot be read, copied, edited or deleted by unauthorized persons while such data is being electronically transferred or while it is being transported or recorded on data media, and that it is possible to check and establish where Personal Data is to be transferred by data transfer equipment.
5. **Measures**: A number of data elements collected by LogicMonitor – including Personal Data – are classified as customer sensitive and handled with utmost care. Specific controls include encryption at rest using AES-256 and encryption in transit using TLS 1.1 or higher with no weak ciphers.

6. Input control. Measures are to be taken to ensure the possibility of verifiable checks and the determination whether Personal Data has been entered, edited or deleted in the DP Systems, and if so by whom.
   a. **Measures**: The only interface LogicMonitor provides for the collection of Personal Data is in the management of user authentication to the service. Any user management actions including creation, modification, and deletion are logged in the account audit log available to all account holders with sufficient access rights.

7. **Order control.** Measures are to be taken to ensure that Personal Data is Processed by Data Importer only in accordance with instructions of the Data Exporter.
    a. **Measures**: LogicMonitor's use of Personal Data is limited to name, email address, and optionally mobile device number. These elements are used within our service only for account management and alert delivery purposes, and these use-cases are enforced by our application code.

8. **Availability control.** Measures are to be taken to ensure that Personal Data is protected against accidental destruction or loss.
    a. **Measures**: In addition to user interface controls protecting data from accidental deletion LogicMonitor maintains continual backups of customer data that form the basis of a rigorous disaster recovery program. Customer backups may be used to restore an environment to correct human error or as part of our disaster recovery processes deployed in case of a facility failure.

9. **Separation control.** Measures are to be taken to ensure that data collected for different purposes can be Processed separately.
    a. **Measures**: LogicMonitor's use of Personal Data is constrained by our application such that it can be used only for account management and alert delivery purposes. All other data collected by LogicMonitor is targeted at monitoring the health and performance of IT systems. The controls that enforce this separation exist within the LogicMonitor codebase.

APPENDIX 3 - SUB-PROCESSORS

Sub-processors. A list of LogicMonitor's Sub-processors is maintained at https://www.logicmonitor.com/data-handling-supplement

Exhibit E

Standard LogicMonitor Employee Background Checks

INTERNATIONAL

Jurisdiction	Search Conducted
United Kingdom	Global Criminal Search (a) (current address of current country of residence only) - Global Education (b) (highest degree)
	7-year Global Employment History - Up to 1 employer (b)
Australia	Global Criminal Search (a) (current address of current country of residence only) - Global Education (b) (highest degree)
	7-year Global Employment History - Up to 1 employer (b)
Other International Locations	Global Criminal Search (a) (current address of current country of residence only) - Global Education (b) (highest degree)
	7-year Global Employment History - Up to 1 employer (b)

DOMESTIC (UNITED STATES)
United States Domestic Services (Applies to 50 United States; excludes US territories and Commonwealths)

Package	Search Conducted
Risk Adverse-US PACKAGE	- SSN Trace - SSN Validation - Criminal Felony & Misdemeanor - 7 years (a) - Unlimited # of counties as revealed by SSN Trace - Widescreen Plus National Criminal Search (g) - National Sex Offender Search
Risk Adverse + Education + Employment	- SSN Trace - SSN Validation - Criminal Felony & Misdemeanor - 7 years (a) - Unlimited # of counties as revealed by SSN Trace - Widescreen Plus National Criminal Search (g) - National Sex Offender Search - Education Report - highest degree(b) - 7 year Employment History - All employers - (b)
Risk Adverse + Education + Up to 3 Employment	- SSN Trace - SSN Validation - Criminal Felony & Misdemeanor - 7 years (a) - Unlimited # of counties as revealed by SSN Trace - Widescreen Plus National Criminal Search (g) - National Sex Offender Search - Education Report - highest degree(b) - 7 year Employment History - Up to 3 employers - (b)

Exhibit F

Operational Resilience Act

1. **Purpose.** This Exhibit F (**"Exhibit"**) supplements the Master Services Agreement, or other signed agreement for the provision of the LogicMonitor Services between the parties (the **"Agreement"**), to ensure the LogicMonitor Services comply with the European Union's Digital Operational Resilience Act (**"DORA"** further defined below). It outlines the enhanced security and privacy practices LogicMonitor will adhere to in delivering the Services to Customers subject to DORA. Except as related to liability and indemnity, this Exhibit will control in the event of a conflict with any terms of the Agreement.

1A. United States & Healthcare Customers: For US-based and healthcare entities, this Exhibit F will be deemed to apply to the Agreement, and any reference to DORA will be read to reference Applicable Law.

2. Definitions.

2.1. "Availability Zones (AZs)" means a data center, or group of data centers with independent power, networking, and housed in separate facilities. AZs are designed to operate independently and are designed such that a failure in one AZ will not result in a failure in another AZ.

2.2. "Critical ICT Third-Party Service Provider (CTPP)" means an ICT third-party service provider designated as critical by the European Supervisory Authorities (ESAs) under the Digital Operational Resilience Act (DORA).

2.3. "DORA" refers to the European Union's Digital Operational Resilience Act, specifically Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, a regulation adopted by the European Union that establishes a comprehensive framework for the digital operational resilience of the financial sector.

2.4. "DORA Audit" or **"DORA Inspection"**

2.5. "Exit Plan" or **"Orderly Exit Window"** means the action plan intended to allow Customer to remove data from the Services, based on realistic and feasible scenarios and assumptions.

2.6. "ICT" stands for information and communication technologies.

2.7. "ICT Risk" means any risk of an event that may negatively impact the operational continuity of LogicMonitor's ICT systems and the Services.

2.8. "Reportable Incident" or simply **"Incident"** has the meaning assigned to it within the Agreement. At a minimum, it refers to any unplanned event that compromises the security of customer's network and information systems, impacting the availability, integrity, confidentiality of data, or the services provided, requiring reporting to relevant authorities if it reaches a "major" severity level based on the impact on critical functions and affected clients.

2.9. **"Recovery Point Objective (RPO)"** means the maximum amount of data loss, measured by time, that the system can lose after a recovery from a disaster, or comparable event. The RPO time is also specified in Section 6 - Disaster Recovery, within the LogicMonitor Security Exhibit.

2.10. **"Recovery Time Objective (RTO)"** means the maximum amount of time that LogicMonitor has to restore operations and the Services after a disaster. The RTO time is also specified in Section 6 - Disaster Recovery, within the LogicMonitor Security Exhibit.

2.11. **(DORA) "Resiliency Objectives"** have the meaning assigned to them as described in Section 6, below**.**

2.12. **"Restricted Data"** has the meaning assigned to it in the Agreement.

2.13. **"Third-Party Audit"** means an audit conducted by a reputable third-party, of LogicMonitor's controls, measures, or effectiveness thereof (as applicable as described in the table below).

2.14. **"Services"** means the LogicMonitor products and services provided to the Customer under the Agreement.

3. DORA Compliance.

3.1. LogicMonitor commits to complying with the relevant provisions of DORA, including but not limited to the following areas:

3.1.1. **Risk Management:** LogicMonitor will maintain a risk management framework to identify, assess, and mitigate ICT risks to the Services. This framework will include regular risk assessments, implementation of appropriate security controls, and ongoing monitoring of the effectiveness of risk mitigation measures.

3.1.2. **Incident Reporting:** LogicMonitor will promptly notify the Customer of any Incidents that may adversely impact the Customer or Customer Data. Such notification will include detailed information about the Incident, its potential impact, and the steps LogicMonitor is taking to mitigate and remediate the Incident. This is further specified in the LogicMonitor Security Exhibit.

3.1.3. **Business Continuity:** LogicMonitor will maintain a comprehensive business continuity and disaster recovery program to ensure the continuous delivery of the Services in the event of disruptive events. This program will include redundant systems, regular backups, and disaster recovery testing. (See below, under Section 6 - Resiliency.)

3.1.4. **Testing:** LogicMonitor will conduct regular testing of its ICT systems and processes with measures designed to ensure their resilience. This testing will include, but not be limited to, penetration testing, vulnerability scanning, and disaster recovery exercises, as described in Table 1 – Testing Methods, below.

3.1.5. **Information Sharing:** LogicMonitor will reasonably cooperate with the Customer and relevant authorities in relation to ICT risks and Incidents. This cooperation will include the timely sharing of information and the coordination of efforts to restore

the Service(s), and reasonable cooperation to mitigate any impact(s) to the Service(s) that are necessary for Customer's DORA compliance.

3.1.6. Exit Plan. Without additional charge to the Customer, in the event of termination of the Agreement, and the applicable Order Form (except in the case of a material breach by Customer), LogicMonitor will provide an Orderly Exit Window of no less than 30 days, with an additional 30 days upon request from Customer, in which Customer may continue use of the LogicMonitor portal solely for the purposes of retrieving Customer Data. LogicMonitor will also provide reasonable cooperation and assistance during the Orderly Exit Window.

Table 1 – Testing Methods

Method / Type	**Description**
Penetration testing	Annual penetration testing is conducted by a reputable third party firm.
Application Security Testing	Ongoing application security testing and scanning will be conducted, and reports will be generated on a documented cadence, with validated defects classified by severity.
Infrastructure scanning / testing	Ongoing infrastructure vulnerability scanning will be conducted on LogicMonitor TechOps-owned compute assets, and reports will be generated and documented on a cadence.
Inapplicable	**Details**
Testing of Covered Account Controls	*Does not apply. The LogicMonitor Services do not process any transactions or maintain covered accounts.*
HIPAA (or similar)	*Does not apply. The LogicMonitor Services do not process any ePHI and are not intended to be used for handling patient data.*

4. Security Governance and Frameworks.

4.1. Strategic Governance; Aligned with Business Needs. LogicMonitor's security framework and written information security policy will be aligned with the organization's overall business strategy and objectives. In addition, LogicMonitor maintains a function for reporting security issues or risks to the board of directors, such as LogicMonitor's cyber risk steering committee, as well as other strategic activities like executive visibility into the risk management program and risk register.

4.2. Documentation. LogicMonitor maintains a documented risk management framework ("RMF") for security and resiliency controls. This RMF is regularly updated and designed to align with external audits undergone by LogicMonitor, such as NIST 800-37 (or similar) or the ISO 27001 framework, and LogicMonitor will make all reasonable efforts to provide relevant information to assist customers in meeting their obligations under DORA.

4.3. Contained in Contract. The parties have entered into the Agreement, which contains the LogicMonitor Security Exhibit. The Security Exhibit describes the applicable frameworks relevant to LogicMonitor's third party auditing activities and written information security policy.

4.4. Code of Conduct. LogicMonitor will maintain a code of conduct for both itself and its business partners, which will remain widely and readily available to the company's employees, contractors, agents, and other staff. LogicMonitor may update these documents from time to time, by modifying the links below.

4.4.1. LogicMonitor Code of Conduct: available at https://www.logicmonitor.com/logicmonitor-code-of-conduct

4.4.2. LogicMonitor Business Partner Code of Conduct: available at https://www.logicmonitor.com/business-partner-code-of-conduct

5. Contractual Obligations

5.1. LogicMonitor will implement measures designed to:

5.1.1. Maintain the security and privacy of Customer Data; and

5.1.2. Comply with all applicable legal and regulatory requirements, including DORA; and

5.1.3. Maintain appropriate technical and organizational security measures; and

5.1.4. Promptly report any Reportable Incident(s) to the Customer (as described in the Security Exhibit); and

5.1.5. Use commercially reasonable efforts to continue all of the current third-party auditing activities, as shown in Table 2 – Applicable Third-Party Audits.

5.1.6. Notify the Customer of material adverse changes to the auditing practices, including stopping a particular audit, unless it is substituted for a newer version of the standards or an improved audit framework.

Table 2 – Applicable Third-Party Audits

Certification/Audit	Description

AICPA SOC2 Type 2	Conducted annually by a third party, available upon request or via the trust center.
ISO/IEC 27001:2013	Confirms LogicMonitor's information security management system meets international standards.
ISO/IEC 27017:2015	Validates LogicMonitor's security controls specific to cloud services.
ISO/IEC 27018:2014	Demonstrates LogicMonitor's commitment to protecting personal data in cloud environments.
Inapplicable	**Details**
N/A - PCI DSS	*No, PCI DSS is not applicable. The LogicMonitor Services do not process any transactions or maintain covered accounts.*
N/A - Covered Account Audit	*No, does not apply. LogicMonitor does not maintain covered account data, manage financial transactions on behalf of a bank, or process payment information.*

5.2 Customer will:

5.2.1 Provide LogicMonitor with timely access to relevant information and systems; and

5.2.2 Promptly notify LogicMonitor of any material compliance issues with DORA and cooperate on a mutually agreeable resolution plan; and

5.2.3 Promptly report any resiliency concerns to LogicMonitor, provided such is necessary to comply with DORA.

6. Resiliency Objectives.

6.1. Recovery Time Objective (RTO) and Recovery Point Objective (RPO). LogicMonitor will implement commercially reasonable measures that are designed to provide service availability as described in the applicable Agreement, and Table 3 – Availability Features, below.

6.2. Additional Availability Objectives.

6.2.1. The RTO, specified in the Agreement, will only apply if more than 1 Availability Zone ("AZ") is impacted.

6.2.2. If the Services are impacted by a single AZ being disrupted, the applicable RTO will be 2 hours from such event.

6.2.3. Where feasible, Supplier strives to maintain three hot copies of all Time Series metric data for customers.

6.3. These Resiliency Objectives do not modify the applicable Uptime and SLA of the MSA, however, these measures are intended to ensure a robust service delivery in the event that LogicMonitor is held to be an third party provider by:

6.3.1. Minimizing the risk of data loss: LogicMonitor has implemented measures designed to ensure that it maintains copies of customer data to ensure that even if one copy is lost or corrupted, others are available. See below for the applicable RPO.

6.3.2. Deploying the platform across multiple AZs: This is intended to ensure that if one AZ is disrupted, the platform can still operate from the other AZs.

6.3.3. Adjusting capacity and distributing workloads across AZs: This helps to maintain optimal performance and availability, even during periods of high demand or disruption.

6.3.4. Utilizing AZs that are physically separated: This is intended to mitigate the risk of simultaneous disruptions caused by localized events, such as natural disasters or power outages.

6.3.5. Providing a shorter RTO in the event of a single AZ disruption: This is designed to ensure that services are restored quickly even in the event of a localized disruption.

Table 2 – Availability Features

Feature	Description
Data Redundancy	Maintain multiple copies of customer data to minimize the risk of data loss.
Multi-AZ Deployment	Deploy the platform across multiple (generally three) AZs within Amazon Web Services (AWS).
Fault Tolerance & Scalability	Adjust capacity and distribute workloads across AZs to maintain optimal performance and availability.

Geographic Dispersion	Utilize AZs that are physically separated to mitigate the risk of simultaneous disruptions caused by localized events (generally by 60 miles).

7. Critical ICT Third-Party Service Providers (CTPPs)

7.1. LogicMonitor and Customer both acknowledge that LogicMonitor does not directly process any transactions, nor maintain any covered accounts, and does not maintain PCI information.

7.2. If LogicMonitor is designated as a CTPP, it will cooperate with LogicMonitor regarding any oversight requirements. This cooperation may include, but is not limited to:

7.2.1. Providing LogicMonitor with timely access to relevant information and systems.

7.2.2. Cooperating with LogicMonitor in the implementation and maintenance of security measures.

7.2.3. Promptly reporting any security concerns or vulnerabilities to LogicMonitor.

7.2.4. Responding to Customer's applicable Overseer, or assisting LogicMonitor in preparing such responses.

7.3. Audits. Customer agrees that the information, questionnaire, assistance, or reasonable cooperation under this Agreement and this Exhibit will satisfy the applicable audit provisions for any CTPP designation of LogicMonitor.

7.4. Edwin AI. Unless explicitly stated otherwise in the applicable Order Form, the parties agree that any Edwin AI Service(s) (if and to the extent applicable) do not support any critical infrastructure, and are not in scope for the Resiliency Objectives.

7.5. No Other Changes. Except as provided under applicable law, but notwithstanding anything else to the contrary, the parties agree that the designation of LogicMonitor as a CTPP will not add additional terms to the Agreement beyond the text of this Exhibit.

8. Training

8.1. LogicMonitor shall provide regular training and awareness programs on ICT risks for its staff. Such training will always include information security and privacy.

8.2. LogicMonitor's training and awareness programs may not necessarily be adapted for each bank or be specific to the banking industry, but are aimed at industry-standard risks.

8.3. No additional training is required by LogicMonitor.