ABNORMAL SECURITY
MASTER CLOUD AGREEMENT

This Master Cloud Agreement ("**Agreement**") is entered into as of the date last executed below ("**Effective Date**") by and between Abnormal Security Corporation, having its principal place of business at 185 Clara Street, Ste 100, San Francisco, CA 94107, United States ("**Abnormal**"), and County of Monterey, on behalf of Natividad Medical Center, having its principal place of business at 1441 Constitution Blvd., Salinas, CA 93906, United States ("**Customer**"). Abnormal and Customer may each be referred to separately as, a "**Party**," or together as, the "**Parties**." This Agreement allows Customer to use Abnormal's Service and receive Support. Capitalized terms are defined in the Section 18 (Glossary) or in context below.

1. ACCESS OF THE SERVICE

1.1. The Service. Subject to this Agreement, Customer may use the Service for its own business purposes during each Subscription Term ("Permitted Use"). This includes the right to copy and use the Documentation as part of Customer's Permitted Use.

1.2. Users. Customer is responsible for provisioning and managing its User accounts, for its Users' actions through the Service and for Users' compliance with this Agreement. Customer will require that Users keep their login credentials confidential and will promptly notify Abnormal upon learning of any compromise of User accounts or credentials.

1.3. Affiliates. Customer's Affiliates may serve as Users. Customer shall be responsible for its Affiliates' use of the Service. Alternatively, Customer's Affiliates may enter into their own Orders as mutually agreed with Abnormal, which creates a separate agreement between each such Affiliate and Abnormal incorporating this Agreement with the Affiliate treated as "Customer". Neither Customer nor any Customer Affiliate has any rights under each other's separate agreement with Abnormal, and breach or termination of any such separate agreement affects only that agreement.

1.4. Support and Availability. Abnormal shall provide Support and adhere to the Service Level Agreement set out in the SLA.

2. DATA

2.1. Customer Data. Customer grants Abnormal a license during each Subscription Term to use Customer Data to provide the Service, Support, and Technical Services to Customer, and to generate Threat Intelligence Data. Use of Customer Data includes sharing Customer Data as Customer directs through the Service, but Abnormal will not otherwise disclose Customer Data to third parties except as permitted in this Agreement.

2.2. Security. Abnormal maintains industry-standard physical, technical, and administrative safeguards as described in the Information Security Policy that are designed to prevent unauthorized access, use, alteration or disclosure of Customer Data.

2.3. Data Processing Addendum; Business Associate Agreement. Abnormal will process Customer Data in accordance with and each Party will comply with, the "Data Processing Addendum" ("DPA") and Business Associates Agreement attached as **Exhibit A**.

2.4. Service Operations Data. Abnormal may collect Service Operations Data and use it to operate, improve and support the Service and for other lawful business purposes, including benchmarking and reports. However, Abnormal will not disclose Service Operations Data externally unless it is (a) de-identified so that it does not identify Customer, its Users or any other person and (b) aggregated with data across other customers.

2.5. Threat Intelligence Data. Abnormal may provide Customer with Threat Intelligence Data regarding the possibility or likelihood of fraudulent, harmful or malicious activity occurring in Customer's environment. Customer understands that Abnormal provides Threat Intelligence Data for Customer's consideration, but that Customer is ultimately responsible for any actions taken or not taken in relation to such Threat Intelligence Data, including any configuration instructions of the Service regarding the level of auto-remediation. Abnormal may incorporate any subsequent action or inaction taken by Customer into its models, for the purpose of identifying future potential fraud, loss, or other harms to customers.

2.6. Third-Party Platforms. Customer may choose to enable integrations or exchange Customer Data with Third-Party Platforms. Customer's use of a Third-Party Platform is governed by its agreement with the relevant provider, not this Agreement, and Abnormal is not responsible for Third-Party Platforms or how Customer's providers use Customer Data.

3. **USE OF THE SERVICE**

3.1. Compliance. Customer will: (a) only use the Service in accordance with the Documentation; and (b) comply with the Acceptable Use Policy and any applicable Product Specific Terms. Customer represents and warrants that it has secured all necessary rights, consents, and permissions to use Customer Data with the Service and grant Abnormal the rights to Customer Data specified in this Agreement, without violating third-party intellectual property, privacy or other rights. Between the Parties, Customer is responsible for the content and accuracy of Customer Data.

3.2. Restrictions. Customer will not (and will use commercially reasonable efforts not to allow any third party to): (a) access or use the Service for any competitive purposes, including to develop a similar or competing product or service (e.g., benchmarking); (b) conduct penetration testing on the Service, interfere with its operation or circumvent its access restrictions; (c) market, sublicense, distribute, resell, lease, loan, transfer, or otherwise commercially exploit or make the Service available (in whole or part) to any third party, except to a third party that manages Customer's computing environment, grant non-Users access to the Service or use the Service to provide a hosted or managed service to others; (d) obtain or attempt to obtain the Service by any means or device with intent to avoid paying the fees that would otherwise be payable for such access or use; or (e) modify, create derivative works of, decompile, reverse engineer, attempt to gain access to the source code of, or copy the Service, or any of its components.

4. **MUTUAL COMPLIANCE WITH LAW.** Each Party will comply with all laws, regulations, court orders or other binding requirements of a government authority ("**Laws**") that apply to its performance under this Agreement.

5. **REPRESENTATIONS AND WARRANTIES**

5.1. Mutual Representations and Warranties. Each Party represents and warrants that:

(a) it has validly entered into this Agreement and has the legal power to do so, and

(b) it will use industry-standard measures to avoid introducing viruses, malicious code or similar harmful materials into the Service.

5.2. Abnormal Warranties. Abnormal warrants that:

(a) the Service shall perform as materially described in the Documentation and Abnormal will not materially decrease the overall functionality of the Service during a Subscription Term (the "**Performance Warranty**"); and

(b) any Technical Services shall be provided in a professional and workmanlike manner (the "**Technical Services Warranty**").

5.3. Abnormal Warranty Remedies. Abnormal shall use commercially reasonable efforts to correct a verified breach of the Performance Warranty or Technical Services Warranty reported by Customer. If Abnormal fails to do so within 30 days after Customer's warranty report, then either Party may terminate the affected Order by giving the other Party a written notice as relates to the non-conforming Service or Technical Services, in which case Abnormal shall refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term (for the Performance Warranty) or for the non-conforming Technical Services (for the Technical Services Warranty). To receive these remedies, Customer must report a breach of warranty in reasonable detail within 30 days after discovering the issue in the Service or 30 days after delivery of the relevant Technical Services. This Section 5.3 sets forth Customer's exclusive remedies and Abnormal's sole liability for breach of the Performance Warranty or Technical Services Warranty.

5.4. Disclaimer. WITH THE EXCEPTION OF THE WARRANTIES SET FORTH IN THIS AGREEMENT, THE SERVICE, SUPPORT, AND TECHNICAL SERVICES ARE PROVIDED "AS IS" TO THE FULLEST EXTENT PERMITTED BY LAW. ABNORMAL AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF PERFORMANCE, MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSES, TITLE AND NON-INFRINGEMENT. WITHOUT LIMITING ITS EXPRESS OBLIGATIONS IN THE SERVICE LEVEL AVAILABILITY COMMITMENT, ABNORMAL DOES NOT WARRANT

THE RESULTS TO BE ACHIEVED FROM THE SERVICE OR THAT THE SERVICE IS ERROR-FREE, WILL PERFORM UNINTERRUPTED OR WILL MEET CUSTOMER'S REQUIREMENTS. THE WARRANTIES IN SECTION 5.2 (ABNORMAL WARRANTIES) DO NOT APPLY TO ISSUES ARISING FROM THIRD PARTY PLATFORMS OR MISUSE OR UNAUTHORIZED MODIFICATIONS OF THE SERVICE. THESE DISCLAIMERS APPLY TO THE FULL EXTENT PERMITTED BY LAW.

6. **TECHNICAL SERVICES.** Abnormal may perform Technical Services as described in an Order, which may identify additional terms or milestones for the Technical Services. Customer will give Abnormal timely access to Customer Materials reasonably needed for Abnormal's provision of the Technical Services, and if Customer fails to do so, Abnormal's obligation to provide Technical Services will be excused until access is provided. Abnormal will use the Customer Materials only for purposes of providing Technical Services. Abnormal may make use of service partners to provide the Technical Services. Subject to any limits in an Order, Customer will reimburse reasonable travel and lodging expenses incurred by Abnormal in providing Technical Services. Customer may use the product of any Technical Services that Abnormal furnishes as part of Technical Services only in connection with Customer's authorized use of the Service under this Agreement.

7. **FEES AND PAYMENT**

7.1. Payment. Customer will pay the fees described in the applicable Order. Unless the Order states otherwise, all undisputed amounts are payable in U.S. dollars and due within 30 days from the date of an invoice ("Due Date"). All fees and expenses are non-refundable and non-cancellable except as expressly set out in the Agreement and any applicable Order.

7.2. Taxes. Customer is responsible for any sales, use, GST, value-added, withholding or similar taxes or levies that apply to its Orders, whether domestic or foreign ("Taxes"), other than Abnormal's income tax. Fees and expenses are exclusive of Taxes. Unless Customer provides Abnormal with a valid exemption certificate, Customer is solely responsible for paying all Taxes associated with or arising from this Agreement.

7.3. Payment Disputes. If Customer disputes an invoice in good faith, it will notify Abnormal prior to the Due Date and the Parties will seek to resolve the dispute over a 15-day discussion period. Customer is not required to pay disputed amounts during the discussion period, but will timely pay all undisputed amounts as agreed in this Agreement. After the discussion period, either Party may pursue any available remedies.

7.4. Records and Validation. Customer is responsible for providing complete and accurate billing and contact information to Abnormal and notifying Abnormal of any changes to such information. Abnormal may conduct verification checks on the usage of the Service during the Subscription Term. If it is determined that the usage of the Service exceeds the baseline quantity stated in an applicable Order, the Parties (Channel Partner and Abnormal or Customer and Abnormal, as applicable) will address any over-usage in a separate Order. If Customer fails to pay for the over-usage, Abnormal may terminate access to the Service within thirty (30) days of Abnormal's written notice of non-compliance.

8. **SUSPENSION.** Abnormal shall be entitled to suspend Customer's access to the Service and related services due to a Suspension Event, but where practicable shall give Customer thirty (30) calendar days written notice so that Customer may seek to resolve the issue and avoid suspension. Abnormal is not required to give prior notice in exigent circumstances or for a suspension made to avoid material harm or violation of Law. Once the Suspension Event is resolved, Abnormal shall promptly restore Customer's access to the Service in accordance with this Agreement. "**Suspension Event**" means (a) Customer's account is thirty (30) days or more overdue; (b) Customer is in breach of Section 3 (Use of the Service) or (c) Customer's use of the Service risks material harm to the Service or others.

9. **TERM AND TERMINATION**

9.1. Subscription Terms. Each Subscription Term will last for an initial 12-month period unless the Order states otherwise. Upon expiration of the applicable Subscription Term, the Parties may renew the Subscription Term for successive periods by entering into a different renewal Order.

9.2. Term. The term of this Agreement will commence on the Effective Date and continues until expiration or termination of all Subscription Terms, unless otherwise terminated as permitted by this Agreement (the "Term"). If no Subscription Term is in effect, either Party may terminate this Agreement for any or no reason with notice to the other Party.

9.3. Termination. Either Party may terminate this Agreement, including all Subscription Terms, if the other Party (a) fails to cure a material breach of this Agreement (including a failure to pay fees) within 30 days after notice, (b) ceases operation

without a successor, or (c) seeks protection under a bankruptcy, receivership, trust deed, creditors' arrangement, composition or comparable proceeding, or if such a proceeding is instituted against that Party and not dismissed within 60 days. Customer shall receive a refund of any pre-paid, unused fees for the terminated portion of an applicable Subscription Term for such Customer-initiated terminations, and Customer will pay Abnormal all undisputed outstanding fees and expenses due pursuant to the payment conditions set forth in this Agreement, both as of the date of termination and for the terminated portion of the Subscription Term for any such Abnormal-initiated termination.

9.4. Data Export & Deletion. During a Subscription Term, Customer may export Customer Data from the Service (or Abnormal will otherwise make the Customer Data available to Customer) as described in the Documentation. After termination or expiration of this Agreement, Abnormal will delete Customer Data and each Party will delete any Confidential Information of the other in its possession or control. Nonetheless, Abnormal may retain Customer Data and each Party may retain Confidential Information in accordance with its standard backup or record retention policies or as required by Law, subject to Section 2.2 (Security), Section 10 (Confidentiality) and the DPA.

9.5. Effect of Termination.

(a) Customer's right to use the Service, Support and Technical Services will immediately cease upon any termination or expiration of this Agreement, subject to this Section 9 (Term and Termination).

(b) In no event will any termination or expiration relieve Customer of the obligation to pay any expenses and fees payable to Abnormal for the period prior to the effective date of termination or expiration.

(c) The following Sections will survive expiration or termination of this Agreement: Section 2.4 (Service Operations Data), 2.5 (Threat Intelligence Data), 3 (Use of the Service), 5.4 (Disclaimers), 7.1 (Payment) (for amounts then due), 7.2 (Taxes), 9.4 (Data Export & Deletion), 9.5 (Effect of Termination), 10 (Confidentiality), 11 (Proprietary Rights), 12 (Limitations of Liability), 13 (Indemnification), 17 (General Terms), and 18 (Glossary).

10. CONFIDENTIALITY

10.1. Use and Protection. As recipient, each Party will (a) use Confidential Information only to fulfill its obligations and exercise its rights under this Agreement, (b) not disclose Confidential Information to third parties without discloser's prior approval, except as permitted in this Agreement, and (c) protect Confidential Information using at least the same precautions recipient uses for its own similar information and no less than a reasonable standard of care.

10.2. Permitted Disclosures. The recipient may disclose Confidential Information to its employees, agents, contractors, Affiliates, subcontractors and other representatives having a legitimate need to know (including, for Abnormal, any subprocessors referenced in the DPA or Service support providers as referenced in Section 17.8) (each, a **"Representative"**), provided recipient remains responsible for their compliance and they are bound to confidentiality obligations no less protective than this Section 10.

10.3. Exclusions. These confidentiality obligations do not apply to information that the recipient can document: (a) is or becomes public knowledge through no fault of the recipient, (b) it rightfully knew or possessed, without confidentiality restrictions, prior to receipt from the discloser, (c) it rightfully received from a third party without confidentiality restrictions or (d) it independently developed without access to the Confidential Information.

10.4. Remedies. Breach of this Section 10 (Confidentiality) may cause substantial harm for which monetary damages are an insufficient remedy. Upon a breach of this Section 10, the discloser is entitled to seek appropriate equitable relief, including an injunction, in addition to other remedies.

10.5. Required Disclosures. The recipient may disclose Confidential Information (including Customer Data) to the extent required by Laws. If a disclosure is permitted, but not required by Law, the recipient will give the discloser reasonable advance written notice of the required disclosure and reasonably cooperate, at the discloser's expense, to contest or seek to limit the disclosure or obtain confidential treatment for the Confidential Information. If no protective order or other remedy is obtained, the recipient will disclose only that portion of the Confidential Information that is legally required, and agrees to exercise reasonable efforts to ensure that confidential treatment will be accorded to such Confidential Information.

11. PROPRIETARY RIGHTS

11.1. Abnormal Property. Abnormal owns and retains all right, title, and interest in and to the Service, Threat Intelligence Data, Technical Services, and any feedback or suggestions Customer provides to Abnormal with respect to the Service or Technical Services. All feedback is provided "AS IS" and Abnormal will not publicly identify Customer as the source of feedback without Customer's written permission. Except for Customer's express rights in this Agreement, as between the Parties, Abnormal and its licensors retain all intellectual property rights in the Service, and product of any Technical Services and related Abnormal technology.

11.2. Customer Property. Except for Abnormal's express rights in this Agreement, as between the Parties, Customer owns and retains all right, title, and interest in and to the Customer Data and Customer Materials provided to Abnormal.

12. LIMITATIONS OF LIABILITY

12.1. General Cap. EACH PARTY'S ENTIRE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL NOT EXCEED THE GENERAL CAP.

12.2. Consequential Damages Waiver. NEITHER PARTY WILL HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR INDIRECT, SPECIAL, INCIDENTAL, RELIANCE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOSS OF USE, LOST PROFITS OR INTERRUPTION OF BUSINESS, EVEN IF INFORMED OF THEIR POSSIBILITY IN ADVANCE.

12.3. Exceptions and Enhanced Cap. SECTIONS 12.1 (GENERAL CAP) AND 12.2 (CONSEQUENTIAL DAMAGES WAIVER) WILL NOT APPLY TO ENHANCED CLAIMS OR UNCAPPED CLAIMS. FOR ALL ENHANCED CLAIMS, EACH PARTY'S ENTIRE LIABILITY WILL NOT EXCEED THE ENHANCED CAP.

12.4. Nature of Claims. The waivers and limitations in this Section 12 (Limitations of Liability) apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy in this Agreement fails of its essential purpose.

12.5. Liability Definitions. The following definitions apply to this Section 12 (Limitations of Liability).

"**Enhanced Cap**" means three times (3x) the General Cap.

"**Enhanced Claims"** means Abnormal's breach of Section 2.2 (Security) or either Party's obligations in or breach of Section 2.3 (DPA).

"**General Cap**" means the total amounts paid and payable by Customer for: (a) use of the Service or (b) performance of the Technical Services, as applicable, to Abnormal under this Agreement in the 12 months immediately preceding the first incident giving rise to a claim of liability. Any Technical Services that are provided on a no-charge basis will be valued at ten thousand dollars for purposes of this definition.

"**Uncapped Claims**" means: (a) the indemnifying Party's obligations under Section 13 (Indemnification); (b) either Party's infringement or misappropriation of the other Party's intellectual property rights; (c) Customer's breach of Section 3.2 (Restrictions; (d) any breach of Section 10 (Confidentiality), excluding breaches related to Customer Data; (e) Customer's payment obligations; (f) Abnormal's gross negligence or willful misconduct and (g) liabilities that cannot be limited by Law.

13. INDEMNIFICATION

13.1. By Abnormal. Abnormal, at its own cost, will defend Customer from and against any Abnormal-Covered Claims and will indemnify Customer from and against any damages or costs finally awarded against Customer by a court of competent jurisdiction (including reasonable attorneys' fees) or agreed in settlement by Abnormal resulting from the Abnormal-Covered Claims.

13.2. By Customer. Customer, at its own cost, will defend Abnormal from and against any Customer-Covered Claims and will indemnify Abnormal from and against any damages or costs finally awarded against Abnormal by a court of competent jurisdiction (including reasonable attorneys' fees) or agreed in settlement by Customer resulting from the Customer-Covered Claims.

13.3. Indemnification Definitions.

"**Abnormal-Covered Claim**" means a third-party claim: (i) that the Service, when used by Customer as authorized in this Agreement, infringes or misappropriates a third party's United States, United Kingdom, or European Union intellectual property rights; or (ii) Abnormal's gross negligence or willful misconducted resulted in personal injury or real and tangible property damage.

"**Customer-Covered Claim**" means a third-party claim arising from Customer Materials or Customer's breach or alleged breach of Section 3 (Use of the Service).

13.4. Procedures. The indemnifying Party's obligations in this Section 13 (Indemnification) are subject to receiving from the indemnified Party: (a) prompt notice of the claim (but delayed notice will only reduce the indemnifying Party's obligations to the extent it is prejudiced by the delay); (b) the exclusive right to control the claim's investigation, defense and settlement; and (c) reasonable cooperation at the indemnifying Party's expense. The indemnifying Party may not settle a claim without the indemnified Party's prior approval if settlement would require the indemnified Party to admit fault or take or refrain from taking any action (except regarding use of the Service when Abnormal is the indemnifying Party). The indemnified Party may participate in a claim with its own counsel at its own expense.

13.5. Mitigation & Exceptions. In response to an infringement or misappropriation claim, if required by settlement or injunction or as Abnormal determines necessary to avoid material liability, Abnormal may, in its sole discretion: (a) procure rights for Customer's continued use of the Service, (b) replace or modify the allegedly infringing portion of the Service to avoid infringement, without reducing the Service's overall functionality or (c) terminate the affected Order or the Agreement and refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term. Abnormal's obligations in this Section 13 (Indemnification) do not apply to claims resulting from (1) modification or unauthorized use of the Service or (2) use of the Service in combination with items not provided by Abnormal, including Third-Party Platforms. This Section 13 (Indemnification) sets out the indemnified Party's exclusive remedy and the indemnifying Party's sole liability regarding third-party claims of intellectual property infringement or misappropriation.

14. INSURANCE

14.1. Abnormal will maintain in full force and effect during the term of this Agreement:

(a) Commercial general liability insurance on an occurrence basis for bodily injury, death, property damage, and personal injury, with coverage limits of not less than US$1,000,000 per occurrence and US$2,000,000 general aggregate for bodily injury and property damage;

(b) Worker's compensation insurance as required by applicable law, including employer's liability coverage for injury, disease and death, with coverage limits of not less than US$1,000,000 per accident and employee;

(c) Umbrella liability insurance on an occurrence form, for limits of not less than US$3,000,000 per occurrence and in the aggregate; and

(d) Technology Errors & Omissions and Cyber-risk insurance on a claims-made form, for limits of not less than US$10,000,000 annual aggregate covering liabilities for financial loss resulting or arising from acts, errors or omissions in the rendering of the Service, or from data damage, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, virus transmission, denial of service, and violation of privacy from network security failures in connection with the Service.

14.2. Insurance carriers will be rated A-VII or better by A.M. Best Provider. To the extent permitted or allowed by its policies, Abnormal's coverage will be considered primary without right of contribution of Customer's insurance policies. In no event will the foregoing coverage limits affect or limit Abnormal's contractual liability, including for indemnification obligations, under this Agreement.

14.3. Unless otherwise specified by this Agreement, all such insurance shall be written on an occurrence basis, or, if the policy is not written on an occurrence basis, such policy with the coverage required herein shall continue in effect for a period of three years following the date Abnormal completes its performance of Services under this Agreement.

Commercial general liability policy shall provide an endorsement naming the County of Monterey, its officers, agents, and employees as Additional insureds with respect to liability arising out of Abnormal's work, including ongoing and completed operations, and shall further provide that such insurance is primary insurance to any insurance or self-insurance maintained by Customer and that the insurance of the Additional Insureds shall not be called upon to contribute to a loss covered by Abnormal's insurance. Blanket endorsements shall be acceptable.

Prior to execution of this Agreement, Abnormal shall provide to Customer's contract administrator and Customer's Contracts Office a "Certificate of Insurance" and individual endorsements showing that Abnormal has in effect the insurance required by this Agreement. Thereafter, upon request by Customer, Abnormal shall make available the certificates of insurance and endorsements to the Customer, showing that Abnormal continues to have in effect the insurance required by this Agreement. Acceptance or approval of insurance shall in no way modify or change the indemnification clause in this Agreement, which shall continue in full force and effect.

15. **TRIALS AND BETAS.** Abnormal may offer optional Trials and Betas. Use of Trials and Betas is permitted only for Customer's internal evaluation during the period designated on the Order (or if not designated in an Order or otherwise, 30 days). Either Party may terminate Customer's use of Trials and Betas at any time for any reason. Trials and Betas may be inoperable, incomplete or include features never released. NOTWITHSTANDING ANYTHING ELSE IN THIS AGREEMENT, ABNORMAL OFFERS NO WARRANTY, INDEMNITY, SLA OR SUPPORT FOR TRIALS AND BETAS AND ITS LIABILITY FOR TRIALS AND BETAS WILL NOT EXCEED US$50,000.

16. **PUBLICITY.** Neither Party may publicly announce this Agreement without the other Party's prior approval or except as required by Laws.

17. **GENERAL TERMS**

17.1. Assignment. Neither Party may assign this Agreement without the prior consent of the other Party, except that either Party may assign this Agreement, with notice to the other Party, to an Affiliate or in connection with the assigning Party's merger, reorganization, acquisition or other transfer of all or substantially all of its assets or voting securities. Any non-permitted assignment is void. This Agreement will bind and inure to the benefit of each Party's permitted successors and assigns.

17.2. Governing Law and Courts. This Agreement is governed by the laws of the State of California without reference to conflicts of law rules. For any dispute relating to this Agreement, the Parties consent to personal jurisdiction and the exclusive venue of the courts in San Francisco County, California.

17.3. Notices.

(a) Except as set out in this Agreement, notices, requests and approvals under this Agreement will be in writing to the addresses on the Order or in this Agreement and will be deemed given: (1) upon receipt if by personal delivery, (2) upon receipt if by certified or registered U.S. mail (return receipt requested), (3) one day after dispatch if by a commercial overnight delivery or (4) upon delivery if by email. Either Party may update its address with notice to the other.

(b) Abnormal may also send operational notices through the Service, including to update the AUP, DPA, ISP, SLA, or other policies to reflect new features or changing practices ("**Referenced Policies**").

17.4. Entire Agreement. This Agreement, inclusive of any Product-Specific Terms, the Referenced Policies, and all applicable Orders, is the Parties' entire agreement regarding its subject matter and supersedes any prior or contemporaneous agreements regarding its subject matter. In this Agreement, headings are for convenience only and "including" and similar terms are to be construed without limitation. Excluding Orders, terms in business forms, purchase orders or quotes, online terms, or invoicing portal used by Customer will not amend or modify this Agreement; any such documents are for administrative purposes only. This Agreement may be executed in counterparts (including electronic copies and PDFs), each of which is deemed an original and which together form one and the same agreement. In the event of any conflict or inconsistency between the Order and this Agreement, the Order will prevail.

17.5. Amendments. Except as permitted under this Agreement, any amendments to this Agreement must be in writing and signed by each Party's authorized representatives.

17.6. Waivers and Severability. Waivers must be signed by the waiving Party's authorized representative and cannot be implied from conduct. If any provision of this Agreement is held invalid, illegal or unenforceable, it will be limited to the minimum extent necessary so the rest of this Agreement remains in effect.

17.7. Force Majeure. Neither Party shall be liable for nonperformance or defective or late performance of any of its obligations under this Agreement to the extent and for such periods of time as such nonperformance, defective performance or late performance is due to reasons outside such Party's reasonable control (a "Force Majeure Event"), including, without limitation, acts of God, war (declared or undeclared), terrorism, action of any governmental authority, civil disturbances, riots, revolutions, vandalism, accidents, fire, floods, explosions, sabotage, nuclear incidents, lightning, weather, earthquakes, storms, sinkholes, epidemics, failure of transportation infrastructure, disruption of public utilities, supply chain interruptions, information systems interruptions or failures, breakdown of machinery or strikes (or similar nonperformance, defective performance or late performance of employees, suppliers or subcontractors); provided, however, that in any such event, each Party shall in good faith use its best efforts to perform its duties and obligations under this Agreement.

If a Party wishes to claim protection with respect to a Force Majeure Event, it shall as soon as possible following the occurrence or date of such Force Majeure Event, notify the other Party of the nature and expected duration of the Force Majeure Event and shall thereafter keep the other Party informed until such time as it is able to perform its obligations. However, this Section does not eliminate Customer's obligations to pay fees owed, subject to the conditions described in this Section 17.7.

17.8. Service Support Providers. Abnormal may use Service support providers (e.g., third-party hosting and other service providers) in provision of the Service and Support and permit them to exercise Abnormal's rights and fulfill Abnormal's obligations, but Abnormal remains responsible for their compliance with this Agreement. This provision does not limit any additional terms for subprocessors under a DPA.

17.9. Independent Contractors. In the performance of work, duties, and obligations under this Agreement, each Party is at all times acting and performing as an independent contractor and not as an agent, partner or joint venturer of the other Party.

17.10. No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.

17.11. Anti-Corruption and Export. Each Party will, and will cause its employees, consultants, and agents to, comply with the US Foreign Corrupt Practices Act of 1977 and the UK Bribery Act 2010. Customer agrees to comply with all applicable laws 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 Laws"), including designated countries, entities, and persons ("Sanctions Targets"); and agrees not to directly or indirectly export, re-export, or otherwise deliver the Service to a Sanctions Target, or broker, finance, or otherwise facilitate any transaction in violation of any Export Laws. Customer represents that Customer is not a Sanctions Target or prohibited from receiving the Service. The Service will be used for non-prohibited, commercial purposes by non-prohibited Users and will not be exported or transferred to China or any Sanctions Target.

17.12. Government Rights. For purposes of this Agreement and to the extent applicable, the Service is "commercial computer software" and a "commercially available off-the-shelf (COTS) item" as defined at FAR 2.101 developed at the private expense of Abnormal. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202 of the DOD FAR Supplement ("DFARS") and its successors. This Section is in lieu of and supersedes any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

17.13. Channel Partner Service Subscriptions. This Section applies to any Customer access of the Service obtained through an authorized Abnormal channel partner (**"Channel Partner"**).

(a) Commercial Terms. Instead of paying Abnormal directly, Customer will pay applicable amounts to the Channel Partner as agreed between Customer and the Channel Partner. Customer's order details (e.g., scope of use, Subscription Term, and fees) will be as stated in the Order placed by Channel Partner with Abnormal on Customer's behalf. Customer's Order will renew with Channel Partner in accordance with Section 9.1 (Subscription Terms), unless Channel Partner notifies Abnormal that it is opting-out of auto-renewal on Customer's behalf as described in this Agreement or in the manner specified in the agreement between Channel Partner and Abnormal. Channel Partner is responsible for the accuracy of such Order. Abnormal may suspend or terminate Customer's rights to use the Service if it does not receive the corresponding payment from the Channel Partner. If Customer is entitled to a refund under this Agreement, Abnormal will refund any applicable fees to the Channel Partner and the Channel Partner will be solely responsible for refunding the appropriate amounts to Customer, unless otherwise specified.

(b) Relationship with Abnormal. This Agreement is directly between Abnormal and Customer and governs all use of the Service by Customer. Channel Partners are not authorized to modify this Agreement or make any promises or commitments on Abnormal's behalf, and Abnormal is not bound by any obligations to Customer other than as set forth in this Agreement. Abnormal is not party to (or responsible under) any separate agreement between Customer and Channel Partner. The amount paid or payable by the Channel Partner to Abnormal for Customer's use of the applicable Service under this Agreement will be deemed the amount paid or payable by Customer to Abnormal under this Agreement for purposes of Section 12 (Limitations of Liability). Abnormal is not responsible for any acts, omissions, products or services provided by Channel Partner.

17.14. Non-Discrimination. During the performance of this Agreement, Abnormal, and its subcontractors, shall not unlawfully discriminate against any person because of race, religious creed, color, sex, national origin, ancestry, physical disability, mental disability, medical condition, marital status, age (over 40), or sexual orientation, either in Abnormal's employment practices or in the furnishing of services to recipients. Abnormal shall ensure that the evaluation and treatment of its employees and applicants for employment and all persons receiving and requesting services are free of such discrimination. Abnormal and any subcontractor shall, in the performance of this Agreement, full comply with all federal, state, and local laws and regulations which prohibit discrimination. The provision of services primarily or exclusively to such target population as may be designated in this Agreement shall not be deemed to be prohibited discrimination.

18. **GLOSSARY.** The definitions of certain capitalized terms used in this Agreement are set forth below. Others are defined in the body of this Agreement.

"**Acceptable Use Policy**" or "**AUP**" means the Acceptable Use Policy attached hereto as **Exhibit D.**

"**Affiliate**" means an entity that directly or indirectly controls, is controlled by, or is under common control with a Party, provided such entity will be considered an Affiliate for only such time as such control interest is maintained; where "**control**" means the ownership of greater than fifty percent (50%) of (a) the voting power to elect directors of the company, or (b) the ownership interests in the company.

"**Confidential Information**" means information disclosed by or on behalf of one Party (as discloser) to the other Party (as recipient) under this Agreement, in any form, which (a) the discloser identifies to recipient as "confidential" or "proprietary" or (b) should be reasonably understood as confidential or proprietary due to its nature and the circumstances of its disclosure. Abnormal's Confidential Information includes the Service, any technical, pricing or performance information about the Service (except pricing information about the Service appearing in this Agreement or amendments thereto), and any information conveyed to Customer in connection with Support. Customer's Confidential Information includes Customer Data and Customer Materials.

"**Customer Data**" means information, including Personal Data (as defined in the DPA), processed by Abnormal via the Service and while providing Support.

"**Customer Materials**" means materials and resources that Customer makes available to Abnormal in connection with Technical Services.

"**Data Processing Addendum**" or "**DPA**" means the Data Processing Addendum attached hereto as **Exhibit B.**

"**Documentation**" means the Abnormal standard technical guides, policies, and documentation for the Service, including all additions and modifications made by Abnormal from time to time, that are made available from the

dedicated 'Documentation' pages within the Service or on the dedicated 'Customer Support' pages of the Abnormal managed website.

"**Force Majeure**" means an unforeseen event beyond a Party's reasonable control, such as a strike, blockade, war, pandemic, act of terrorism, riot, third-party Internet, telecommunications or utility failure, acts or orders of government, refusal of government license or natural disaster, where the affected Party takes reasonable and customary measures to avoid or mitigate such event's effects.

"**Information Security Policy**" or "**ISP**" means the Information Security Policy attached hereto as **Exhibit C.**

"**Order**" means an order for Customer's access to the Service, Support, or Technical Services or related services that is: (a) either executed by the Parties and references this Agreement or entered into by Customer via self-service; or (b) entered into by Abnormal and a Channel Partner on behalf of Customer.

"**Product Specific Terms**" means any terms and conditions specific to an applicable Service that supplement, but do not replace, this Agreement and are available at legal.abnormalsecurity.com.

"**Service**" means Abnormal's proprietary software-as-a-service products, as identified in the relevant Order, including any modifications, updates, upgrades, and enhancements thereto that Abnormal makes generally available to its customer base. The Service includes the Documentation but not Technical Services or Third-Party Platforms.

"**Service Operations Data**" means Abnormal's technical logs, analytics or other data and learnings related to Customer's use of the Service, but excluding Customer Data.

"**Service Level Agreement**" or "**SLA**" means the Support and Service Level Policy attached hereto as **Exhibit E.**

"**Subscription Term**" means the term for Customer's use of the Service as set forth on the applicable Order.

"**Support**" means the customer support services set out on: (a) the dedicated 'Customer Support' page of the Abnormal website, and (b) the SLA; but excludes any Technical Services.

"**Technical Services**" means training, migration, enablement or other technical services that Abnormal furnishes to Customer related to the Service.

"**Threat Intelligence Data**" means information collected, generated, derived, and/or analyzed by the Service that is related to malicious activities, fraud, loss, threat or other harm detection and analysis identified by the Service such as a third-party malicious actor's IP address, email address, name, and hashes of malware.

"**Third-Party Platform**" means any product, add-on or platform not provided by Abnormal that Customer uses with the Service.

"**Trials and Betas**" mean access to the Service (or Service features) on a free, trial, beta or early access basis.

"**Users**" means individuals or entities that are authorized by Customer to use the Service under its account and on its behalf.

The Parties have caused this Agreement to be executed by their duly authorized representatives.

ABNORMAL SECURITY CORPORATION

Signature: DocuSigned by: Preston Graham 03B124F53EB64B9...

Name: Preston Graham

Title: Controller of Finance

Date: 4/1/2025 | 1:54 PM PDT

Address: 8474 Rozita Lee Ave, Suite 420, Las Vegas NV 89113, United States

Signature: DocuSigned by: Kevin Johnson 50A0065D78E24CE...

Name: Kevin Johnson

Title: Deal Desk

Date: 4/1/2025 | 2:23 PM PDT

Address: 8474 Rozita Lee Ave, Suite 420, Las Vegas NV 89113, United States

COUNTY OF MONTEREY, on behalf of NATIVIDAD MEDICAL CENTER

Signature:

Name: Charles R. Harris

Title: CEO

Date:

Address: 1441 Constitution Blvd., Salinas, CA 93906, United States

APPROVED AS TO LEGAL PROVISIONS

Signature: Signed by: Stacy Saetta 696D21D44C4341D...

Name: Stacy Saetta

Title: Monterey County Deputy County Counsel

Date: 4/2/2025 | 5:40 PM PDT

APPROVED AS TO FISCAL PROVISIONS

Signature:

Name: Auditor/Controller Signers

Title: Monterey County Deputy Auditor/Controller

Date:

Exhibit A
Abnormal Security
HIPAA Business Associate Agreement

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data, this HIPAA Business Associate Agreement ("**BAA**") is incorporated into and forms part of the agreement for Customer's use of Abnormal's services upon the effective date the Abnormal Security Master Cloud Agreement is entered into by and between the entity identified as Customer on the signature page ("**Customer**") and Abnormal ("**Agreement**"). If and to the extent there is any conflict between a provision in this BAA and a provision in the Agreement, this BAA will control.

1. Definitions.

Except as otherwise defined in this BAA, capitalized terms shall have the definitions set forth in HIPAA, and if not defined by HIPAA, such terms shall have the definitions set forth in the Agreement.

"Breach Notification Rule" means the Breach Notification for Unsecured Protected Health Information Final Rule.

"Business Associate" shall have the same meaning as the term "business associate" in 45 CFR § 160.103 of HIPAA.

"Covered Entity" shall have the same meaning as the term "covered entity" in 45 CFR § 160.103 of HIPAA.

"Customer", for this BAA only, means Customer and its Affiliates.

"HIPAA" collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health ("HITECH") Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

"Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information.

"Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103 of HIPAA, provided that it is limited to such protected health information that is received by Abnormal from, or created, received, maintained, or transmitted by Abnormal on behalf of, Customer through the use of the Service.

"Security Rule" means the Security Standards for the Protection of Electronic Protected Health Information.

"Technical Services" means training, migration or other professional services that Abnormal furnishes to Customer related to the Service.

2. Permitted Uses and Disclosures of Protected Health Information.

a. Performance of the Agreement. Except as otherwise limited in this BAA, Abnormal may Use and Disclose Protected Health Information for, or on behalf of, Customer as specified in the Agreement; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted under paragraph b of this Section.

b. Management, Administration, and Legal Responsibilities. Except as otherwise limited in this BAA, Abnormal may Use and Disclose Protected Health Information for the proper management and administration of the Service and/or to carry out Abnormal's legal responsibilities, provided that any Disclosure may occur only if: (1) Required by Law; or (2) Abnormal obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Abnormal of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

3. Responsibilities of the Parties with Respect to Protected Health Information.

a. Abnormal's Responsibilities. To the extent Abnormal is acting as a Business Associate, Abnormal agrees to the following:

(i) **Limitations on Use and Disclosure.** Abnormal shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this BAA or as otherwise Required by Law. Abnormal shall not disclose, capture, maintain, scan, index, transmit, share or Use Protected Health Information for any activity not authorized under the Agreement and/or this BAA. The Service and Technical Services shall not use Protected Health Information for any advertising, Marketing or similar commercial purpose of Abnormal or any third party. Abnormal shall not violate the HIPAA prohibition on the sale of Protected Health Information. Abnormal shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.

(ii) **Safeguards.** Abnormal shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.

(iii) **Reporting.** Abnormal shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Abnormal becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer's Unsecured Protected Health Information that Abnormal may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, but in no event later than five business days after Abnormal's discovery of a Breach. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting will be made consistent with Abnormal's and Customer's legal obligations.

For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on Abnormal's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Customer pursuant to Section 3b(ii) (Contact Information for Notices) of this BAA by any means Abnormal selects, including through e-mail. Abnormal's obligation to report under this Section is not and will not be construed as an acknowledgement by Abnormal of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

(iv) **Subcontractors.** In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Abnormal shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Abnormal to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Abnormal with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule. Abnormal remains responsible for its Subcontractors' compliance with obligations in this BAA.

(v) **Disclosure to the Secretary.** Abnormal shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Customer to the Secretary of the Department of Health and Human Services for purposes of determining Customer's compliance with HIPAA, subject to attorney-client and other applicable legal privileges. Abnormal shall respond to any such request from the Secretary by redirecting the Secretary to request that information directly from the Customer. If compelled to disclose or provide access to such information, Abnormal will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so. In support of the above, Abnormal may provide Customer's basic contact information to the third party.

(vi) **Access.** The parties acknowledge and agree that Abnormal does not maintain Protected Health Information in a Designated Record Set for Customer. In the event that there is a change in the Service that Abnormal provides to Customer such that Abnormal commences maintaining Protected Health Information in a Designated Record Set, then Abnormal, at the request of Customer, shall within fifteen (15) days make access to such Protected Health Information available to Customer in accordance with 45 CFR § 164.524 of the Privacy Rule.

(vii) **Amendment.** Subject to Section 3a(vi) above, if Abnormal maintains Protected Health Information in a Designated Record Set for Customer, then Abnormal, at the request of Customer, shall within fifteen (15)

days make available such Protected Health Information to Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.

(viii) Accounting of Disclosure. Abnormal, at the request of Customer, shall within thirty (30) days make available to Customer such information relating to Disclosures made by Abnormal as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

(ix) Performance of a Covered Entity's Obligations. To the extent Abnormal is to carry out a Covered Entity obligation under the Privacy Rule, Abnormal shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.

b. Customer Responsibilities.

(i) No Impermissible Requests. Customer shall not request Abnormal to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).

(ii) Contact Information for Notices. Customer hereby agrees that any reports, notification, or other notice by Abnormal pursuant to this BAA will be provided as set forth in the Agreement.

(iii) Safeguards and Appropriate Use of Protected Health Information. Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Customer's obligation to:

1) Not include Protected Health Information in: (1) information Customer submits to technical support personnel through a technical Support request or to community support forums, or, for Technical Services; (2) clear text in email data stores; and (3) Customer's address book or directory information. In addition, Abnormal does not act as, or have the obligations of, a Business Associate under HIPAA with respect to Customer Data once it is sent to or from Customer outside the Service or Technical Services over the public Internet, or if Customer fails to follow applicable instructions regarding physical media transported by a common carrier.

2) During use of the Service or in an engagement with Abnormal to obtain Technical Services, implement privacy and security safeguards in the systems, applications, and software that Customer controls, configures, and uploads.

4. Applicability of BAA.

This BAA is applicable to the Service and Technical Services. Abnormal may, from time to time, (a) include additional features in the Service, and (b) update the definition of the Service and Technical Services in this BAA, and such updated definitions will apply to Customer without additional action by Customer. It is Customer's obligation to not store or process in an online service, or provide to Abnormal for performance of a professional service, protected health information (as that term is defined in 45 CFR § 160.103 of HIPAA) until this BAA is effective as to the applicable service.

5. Term and Termination.

a. Term. This BAA shall continue in effect until the earlier of (1) termination by a Party for breach as set forth in Section 5.b., or as set forth in Section 5.c. below, or (2) expiration of Customer's Agreement.

b. Termination. Upon written notice, either Party may immediately terminate the Agreement and this BAA if the other Party is in material breach of any obligation in this BAA. Either Party may provide the other a thirty (30) calendar day period to cure a material breach or default within such written notice. Either party has the right to terminate this BAA for any reason upon 12 months' prior written notice to the other party.

c. End of Life. Abnormal will provide at least 12 months' prior notice to Customer if Abnormal decides to remove an existing Service or existing functionality of a Service covered by this BAA, which Abnormal may do so notwithstanding anything in this BAA or the Agreement and without penalty. Abnormal will not be obligated to provide notice under the prior sentence if the removal is necessary to address an emergency or threat to the security or integrity of Abnormal or its suppliers, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or requests of a government entity. Where

Abnormal is excused from providing notice under the prior sentence, Abnormal will use commercially reasonable efforts to provide as much advance notice as is reasonably practicable under the circumstances (which Customer acknowledges may be no prior notice).

d. Return, Destruction, or Retention of Protected Health Information Upon Termination. Upon expiration or termination of this BAA, Abnormal shall return or destroy all Protected Health Information in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement. If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA, then Abnormal shall extend the protections of this BAA, without limitation, to such Protected Health Information and limit any further Use or Disclosure of the Protected Health Information to those purposes that make the return or destruction infeasible for the duration of the retention of the Protected Health Information.

6. **Customer acknowledgement**

a. Acknowledgement of Abnormal's Service. Customer covenants and warrants it will not send Designated Record Sets, substantial portions of Designated Record Sets, or any other health records in full to Abnormal, or use the Service as a personal health record for patients.

7. ***Miscellaneous.***

a. Interpretation. The Parties intend that this BAA be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state law. Except where and to the extent this BAA conflicts with the Agreement, all other terms and conditions of the Agreement remain unchanged. Any captions or headings in this BAA are for the convenience of the Parties and shall not affect the interpretation of this BAA. Any claims of Breach brought under or in connection with this BAA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations and considered as an Enhanced Claims as set forth in the Agreement.

b. Amendments; Waiver. This BAA may not be modified or amended except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, as a bar to, or as a waiver of any right or remedy as to subsequent events.

c. No Third-Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor shall anything in this BAA confer, upon any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

d. Severability. In the event that any provision of this BAA is found to be invalid or unenforceable, the remainder of this BAA shall not be affected thereby, but rather the remainder of this BAA shall be enforced to the greatest extent permitted by law.

e. No Agency Relationship. It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Customer and Abnormal under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms or conditions contained in this BAA shall be construed to make or render Abnormal an agent of Customer.

Exhibit B

Abnormal Security

Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements and is incorporated into the Agreement.

1. Definitions. The definitions of certain capitalized terms used in this DPA are set forth below. Others are defined in the body of the DPA. Capitalized terms not defined in this DPA are defined in the Agreement.

1.1. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

1.2. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder and the California Privacy Rights Act of 2020 (collectively, the "**CCPA/CPRA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

1.3. "**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

1.4. "**EEA**" means European Economic Area.

1.5. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.6. "**Privacy Data Sheet**" means the applicable document, if and when made available on the Abnormal Trust Portal and incorporated by reference into this DPA, that describes the Processing activities in relation to the specific Service supplied to Customer under the Agreement.

1.7. "**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.8. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.9. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Personal Data from the United Kingdom to any country that is not subject to an adequacy determination, or (iii) where FADP applies, a transfer of Personal Data from Switzerland to any country that is not subject to an adequacy determination.

1.10. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data being Processed by Abnormal.

1.11. "**Specified Notice Period**" is 48 hours.

1.12. "**Subprocessor**" means any third party authorized by Abnormal to Process any Personal Data.

1.13. "**Subprocessor List**" means the list of Abnormal's Subprocessors as referred to in Section 4.2 (Subprocessor List) below.

1.14. "**Trust Portal**" means https://security.abnormalsecurity.com/.

2. Scope and Duration.

2.1. Roles of the Parties. This DPA applies to Abnormal as a Processor of Personal Data and to Customer as a Controller or Processor of Personal Data.

2.2. Scope of DPA. This DPA applies to Abnormal's Processing of Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. Duration of DPA. This DPA commences on the Agreement Effective Date and terminates upon expiration or termination of the Agreement (or, if later, the date on which Abnormal has ceased all Processing of Personal Data).

2.4. Order of Precedence. Any ambiguity, conflict or inconsistency between this DPA, the Agreement, the Abnormal Information Security Policy, or any other document comprising the Agreement shall be resolved according to the following order of precedence: (1) any Standard Contractual Clauses or other measures to which the Parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA, (3) the Information Security Policy, (4) the Agreement, and (5) other supplementary documents incorporated into the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. Customer Instructions.

(a) Abnormal will Process Personal Data as a Processor only: (i) in accordance with Customer Instructions, or (ii) to comply with Abnormal's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Customer Instructions**" means: (i) Processing to provide the Service and as described in the Agreement (including this DPA and the applicable Privacy Data Sheet) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

(c) Details regarding the Processing of Personal Data by Abnormal are set forth in Schedule 1 (Subject Matter and Details of Processing) and the applicable Privacy Data Sheet.

(d) Abnormal will notify Customer if it receives an instruction that Abnormal reasonably determines infringes Data Protection Laws (but Abnormal has no obligation to actively monitor Customer's compliance with Data Protection Laws). In such an instance, Abnormal will be entitled to suspend performance of such instruction, until Customer confirms in writing that such instruction is valid under Data Protection Laws.

3.2. Confidentiality.

(a) Abnormal will protect Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Abnormal will ensure personnel who Process Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. Compliance with Laws.

(a) Abnormal and Customer will each comply with Data Protection Laws in their respective Processing of Personal Data.

(b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Abnormal. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Abnormal to lawfully Process Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects. Customer is solely responsible for ensuring the accuracy, quality, and legality of Personal Data Processed by Abnormal including the means by which Customer acquired Personal Data.

3.4. Changes to Laws. The Parties will work together in good faith to negotiate an amendment to this DPA as either Party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. Subprocessors.

4.1. Use of Subprocessors.

(a) Customer generally authorizes Abnormal to engage Subprocessors to Process Personal Data. Customer further agrees that Abnormal may engage its Affiliates as Subprocessors.

(b) Abnormal will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Abnormal to breach any of its obligations under this DPA.

4.2. Subprocessor List. Abnormal will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the Subprocessor List set forth in Schedule 1 or the applicable Privacy Data Sheet.

4.3. Notice of New Subprocessors. Abnormal may update the Subprocessor List from time to time. At least 30 days before any new Subprocessor Processes any Personal Data, Abnormal will add such Subprocessor to the Subprocessor List and notify Customer through email or other means.

4.4. Objection to New Subprocessors.

(a) If, within 30 days after notice of a new Subprocessor, Customer notifies Abnormal in writing that Customer objects to Abnormal's appointment of such new Subprocessor based on reasonable data protection concerns, the Parties will discuss such concerns in good faith.

(b) If the Parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Order for the affected Service for convenience and Abnormal will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

5. Security.

5.1. Security Measures. Abnormal will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Personal Data and protect against Security Incidents, in accordance with Abnormal's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Abnormal will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. Incident Notice and Response.

(a) Abnormal will implement and follow procedures to detect and respond to Security Incidents.

(b) Abnormal will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Abnormal's reasonable control.

(c) Upon Customer's request and taking into account the nature of the applicable Processing, Abnormal will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

(d) Customer acknowledges that Abnormal's notification of a Security Incident is not an acknowledgement by Abnormal of its fault or liability.

(e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. Customer Responsibilities.

(a) Customer is responsible for reviewing the information made available by Abnormal relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws.

(b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. Data Protection Impact Assessment. Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Abnormal, Abnormal will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment

related to Customer's use of the Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. Data Subject Requests.

7.1. Assisting Customer. Upon Customer's request and taking into account the nature of the applicable Processing, Abnormal will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Service).

7.2. Data Subject Requests. If Abnormal receives a request from a Data Subject in relation to the Data Subject's Personal Data, Abnormal will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. Data Return or Deletion.

8.1. During Subscription Term. During the Subscription Term, Customer may, through the features of the Service or such other means, access, return to itself or delete Personal Data.

8.2. Post Termination.

(a) Following termination or expiration of the Agreement, Abnormal will, in accordance with its obligations under the Agreement, delete all Personal Data from Abnormal's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Abnormal will issue a certificate of deletion upon Customer's request.

(c) Notwithstanding the foregoing, Abnormal may retain Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Abnormal will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Personal Data and (y) not further Process retained Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. Audits.

9.1. Abnormal Records Generally. Abnormal will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Abnormal's obligations under this DPA and Data Protection Laws.

9.2. Third-Party Compliance Program.

(a) Abnormal will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (but not more than once annually) (subject to confidentiality obligations).

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.

9.3. Customer Audit. Abnormal will make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Service. To this end, upon written request (not more than once annually) Customer may, at its sole cost and expense, verify Abnormal's compliance with its data protection obligations as specified in this DPA by: (i) submitting a security assessment questionnaire to Abnormal; and (ii) if Customer is not satisfied with Abnormal's responses to the questionnaire, then Customer may conduct an audit in the form of meetings with Abnormal's information security experts on a mutually agreeable date. Such interviews will be conducted with a minimum of disruption to Abnormal's normal business operations and subject to Abnormal's agreement on scope and timing. Customer may perform the verification described above either itself or by a mutually agreed upon third party auditor, provided that Customer or its authorized auditor executes a mutually agreed upon non-disclosure agreement. Customer will be responsible for any actions taken by its authorized auditor. All information disclosed by Abnormal under this Section 9.3 will be deemed Abnormal Confidential Information, and

Customer will not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency. Abnormal will remediate any mutually agreed, material deficiencies in its technical and organizational measures identified by the audit procedures described in this Section 9.3 within a mutually agreeable timeframe.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. Cross-Border Data Transfers.

(a) Abnormal (and its Affiliates) may Process and transfer Personal Data globally as necessary to provide the Service.

(b) If Abnormal engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. Region-Specific Terms. To the extent that Abnormal Processes Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

Schedule 1 – Subject Matter and Details of Processing

Customer may subscribe in the Trust Portal to receive email notifications with detailed information about certain updates to the processing operations of the Abnormal Service, including as published in the applicable Privacy Data Sheet(s). By clicking on the "Subscribe" link located in the upper right-hand corner of the Trust Portal, Customer will receive an email notification when an update in the Trust Portal is made.

A. LIST OF PARTIES

Data exporter(s):

Name:	The named "Customer" on the signed or accepted Order or Agreement.
Address:	The address associated with the Customer on the signed or accepted Order or Agreement.
Contact person's name, position and contact details:	The contact details associated with the Customer on the signed or accepted Order or Agreement.
Activities relevant to the data transferred under these Clauses:	See Description of Transfer below.
Signature and date:	Refer to the signed or accepted Order or Agreement.
Role (controller/processor):	Controller

Data importer(s):

Name:	Abnormal Security Corporation
Address:	185 Clara Street, Suite 100, San Francisco, CA 94107, United States
Contact person's name, position and contact details:	The contact details associated with Abnormal on the signed or accepted Order or Agreement.
Activities relevant to the data transferred under these Clauses:	See Description of Transfer below.
Signature and date:	Refer to the signed or accepted Order or Agreement.
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Individual users of the cloud office applications and infrastructure that Controller has authorized Processor's Service to connect to, including Controller's messaging systems, as well as individuals sending messages to or receiving messages from user accounts.
Categories of personal data transferred	● Personal Data contained in message content

	and file attachments ● User information including user name, roles, email, group assignments, and configuration settings ● Personal Data contained within activity logs, audit logs, and administrator reports (e.g. user id, IP address) More detailed categories of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	N/A
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Ongoing as determined by the Controller.
Nature of the processing	For the provision of the Service and Support under the Agreement. More details on Abnormal processing activities of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal.
Purpose(s) of the data transfer and further processing.	Scanning of message contents, metadata, activity logs, and cloud application and infrastructure configurations for malicious activity and signatures. More detailed purposes for Abnormal processing of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.	During the Term and as set forth in the data retention policies as published in the Documentation. Additional specific retention periods for Abnormal processing of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal.
For transfers to (sub-) processors, also specify subject matter, nature and duration	During the Term and as specified under the Agreement.

of the processing.	

C. SUBPROCESSORS

The Controller has authorised the use of the following Subprocessors: The Subprocessors located on the agreed list available at www.abnormalsecurity.com/trust, the Abnormal Trust Portal, and as published in the applicable Privacy Data Sheet.

Schedule 2 – Technical and Organizational Measures

Abnormal has taken and will maintain the appropriate administrative, technical, physical and procedural security measures, for the protection of the Personal Data, including the measures set forth below or otherwise made reasonably available by Abnormal. Further up-to-date Service specific technical and organisational measures will be as set out in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal.

Policy Controls:

- Abnormal has established an information security policy that is reviewed and approved on a regular cadence.
- A framework of security standards has been developed, which supports the objectives of the security policy.
- Procedures and systems exist for requesting, establishing, issuing, suspending, deleting, and closing user accounts and associated access privileges, e.g. system access is granted based upon position, job function, and manager approval.
- Access to Abnormal offices is controlled via card key access, and is under 24/7 CCTV monitoring.
- No Customer Data is stored on Abnormal premises.

Collection of Data:

- The Service processes Customer Data on an in-memory basis via API.
- Customer Data that is processed and identified as malicious by the Service is transferred to Abnormal servers that support the Service and stored for the period set forth in Abnormal's data retention policies as published in the Documentation. Such data is then automatically deleted at the end of such period.
- All Customer Data is encrypted at rest using multi-factor encryption with a per-file key and AES-256 block cipher, with keys managed by a secured key management service.

Backup Copies:

- Procedures for backup and retention of data and programs have been documented and implemented.
- Backups are encrypted and access is limited based upon least privilege.
- Data and programs are backed up regularly and tested to ensure recoverability.

Computers and Access Terminals:

- New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
- Employees are required to acknowledge receipt of Abnormal’s Information Security Policy.
- Access to the production environment is authorized by the appropriate management and is based on least privilege and business need. A multi-factor secure remote access is required for all access to the production systems.
- All print services are disabled by default on all production servers

Access Controls:

- All Abnormal employees and contractors are provided with unique userIDs
- Access is only granted to employees whose role requires it.
- Access is disabled upon role reassignment or termination.
- Access is revoked on termination.
- Multi-Factor Authentication, including biometric fingerprint verification, is required to access Abnormal systems and Customer Data.

Security while transferring and processing:

- Segmentation of network environment using logical networking controls.
- Default blocked firewall policies.
- Limited number of integration-related endpoints are accessible via public internet and protected by Web Application Firewall (WAFs).
- Public endpoints utilize Application Load Balancers, and are resilient to dynamic changes in query load/throughput
- Data in transit encrypted using TLS 1.2 sessions with a 2048-bit RSA asymmetric key.

- HTTPS required for all web traffic.
- Encrypted connectors for databases using SSL.

Schedule 3 – Cross-Border Transfer Mechanism

1. Definitions. Capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

1.3. In addition:

"**Designated EU Governing Law**" means:	The laws of the Republic of Ireland
"**Designated EU Member State**" means:	Republic of Ireland

2. EU Transfers. Where Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

2.1. The EU SCCs are hereby incorporated by reference as follows:

(a) Module 2 (Controller to Processor) applies where Customer is a Controller of Personal Data and Abnormal is a Processor of Personal Data;

(b) Module 3 (Processor to Processor) applies where Customer is a Processor of Personal Data (on behalf of a third-party Controller) and Abnormal is a Processor of Personal Data;

(c) Customer is the "data exporter" and Abnormal is the "data importer"; and

(d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.

2.2. For each Module, where applicable the following applies:

Section Reference	Selection by the Parties
Section I, Clause 7	The docking clause does not apply.
Section II, Clause 9	Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Abnormal shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA.
Section II, Clause 11	The optional language does not apply.
Section II, Clause 13	All square brackets are removed with the text remaining.
Section IV, Clause 17	Option 1 will apply, and the EU SCCs will be governed by the Designated EU Governing Law.
Section IV, Clause 18 (b)	Disputes will be resolved before the courts of the Designated EU Member State.
Schedule 1 (Subject Matter and Details of Processing)	Contains the information required in Annex 1 of the EU SCCs.
Schedule 2 (Technical and Organisational Measures)	Contains the information required in Annex 2 of the EU SCCs.

2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

3. Swiss Transfers. Where Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

Section Reference	Selection by the Parties

Section II, Clause 13	The competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.
Section IV, Clause 17 (Option 1)	The EU SCCs will be governed by the laws of Switzerland.
Section IV, Clause 18 (b)	Disputes will be resolved before the courts of Switzerland.
Section IV, Clause 18 (c)	The term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).
EU GDPR	All references to the EU GDPR in this DPA are also deemed to refer to the FADP.

4. **UK Transfers**. Where Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) each party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Personal Data;

(c) in Table 1 of the UK Addendum, the parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;

(e) in Table 3 of the UK Addendum:

(i) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(ii) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and

(iv) the list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.

(f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(g) in Part 2: Part 2 - Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

Schedule 4: Region-Specific Terms

A. CALIFORNIA

1. Definitions. CCPA/CPRA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA/CPRA.

1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA/CPRA.

1.3. The definition of "Controller" includes "business" as defined under the CCPA/CPRA.

1.4. The definition of "Processor" includes "service provider" as defined under the CCPA/CPRA.

2. Obligations.

2.1. Customer is providing the Personal Data to Abnormal, acting as a service provider, under the Agreement for the limited and specific business purposes of providing the Service as described in Schedule 1 (Subject Matter and Details of Processing) to this DPA or the applicable Privacy Data Sheet, and otherwise performing under the Agreement.

2.2. Abnormal will comply with its applicable obligations under the CCPA/CPRA and provide the same level of privacy protection to Personal Data as is required by the CCPA/CPRA.

2.3. Abnormal acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Abnormal use of Personal Data is consistent with Customer's obligations under the CCPA/CPRA, (ii) receive from Abnormal notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA/CPRA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

2.4. Abnormal will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA/CPRA.

2.5. Absent Customer Instructions or the Customer's prior written agreement, or generating Threat Intelligence Data, Abnormal will not retain, use or disclose Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.1 of this Section A (California) of Schedule 4 and generating Threat Intelligence Data, or (ii) outside of the direct business relationship between Abnormal with Customer, except, in either case, where and to the extent permitted by the CCPA/CPRA.

2.6. Abnormal will not sell or share Personal Data received under the Agreement.

2.7. Abnormal will not combine Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA/CPRA.

EXHIBIT C

ABNORMAL SECURITY CORPORATION INFORMATION SECURITY POLICY

This Information Security Policy ("**Policy**") is incorporated into the subscription agreement under which Abnormal Security Corporation ("Abnormal", "we", or "us") provides its Service ("**Agreement**") to the Party listed as Customer on the Agreement ("**Customer**") and describes Abnormal's Information Security Program ("**Security Program**") which Abnormal has implemented and will maintain in accordance with this Policy.

Abnormal may update this Policy from time to time, provided that any such update does not: (i) modify any provision of the Agreement except for this Policy; or (ii) materially diminish the overall security protections described herein during the Subscription Term. Any such updates will be posted to https://legal.abnormalsecurity.com/. Capitalized terms not otherwise defined in this Policy shall have the meanings given to them in the Agreement. Any ambiguity, conflict or inconsistency between this Policy, the Agreement, the DPA, or other document comprising this Agreement shall be resolved according to the following order of precedence: (1) DPA; (2) this Policy; (3) the Agreement; and (4) other supplementary documents incorporated into the Agreement.

Minimum Security Standards. The Security Program will use industry-standard controls designed to protect the confidentiality, integrity, and availability of Customer Data against anticipated or actual threats or hazards; accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or damage. The Security Program will use administrative, technical, and physical safeguards appropriate to: (a) the size, scope, and type of Abnormal's business; (b) the type of information that Abnormal processes on behalf of Customer (where such information is provided to Abnormal in accordance with the Agreement); and (c) the corresponding need for security and confidentiality of such information.

For more details on Abnormal's Security Program, please see the Security Hub at security.abnormalsecurity.com ("**Security Hub**").

Service Infrastructure. The Service and Customer Data are hosted on infrastructure using industry-leading cloud hosting providers. No Customer Data is stored or processed in Abnormal office facilities.

Elements of the Security Program.

1. Policies and Procedures. Abnormal has implemented and will maintain security, privacy, confidentiality, availability, and code of conduct policies and procedures designed to ensure that the Service and Abnormal's employees and contractors ("**Personnel**") process Customer Data in accordance with this Policy and the Agreement. Abnormal has implemented and will enforce disciplinary measures against Personnel for failure to abide by the aforementioned policies and procedures.

2. Logical Access Controls. Abnormal will take reasonable measures that are designed to ensure appropriate user authentication for Personnel with access to Customer Data, including without limitation, by assigning each Personnel unique authentication credentials for accessing any system on which Customer Data is processed and prohibiting Personnel from sharing their authentication credentials. Abnormal will restrict access to Customer Data solely to those Personnel who need access to Customer Data to perform Abnormal's obligations under the Agreement.

Further, Abnormal will take reasonable measures to implement and maintain logging and monitoring technologies designed to help detect and prevent unauthorized access to its networks, servers, and applications, including but not limited to those that process Customer Data. Abnormal will conduct periodic reviews of systems that process Customer Data to verify the identities of individuals who access and have privileged access to systems to help detect and prevent unauthorized access to its network, servers, and applications and verify that all changes to its authentication systems were authorized and correct. Abnormal has implemented and will maintain procedures and policies that are designed to ensure that, upon termination of any Personnel the terminated user access to any Customer Data on Abnormal systems will be promptly revoked, and in all cases, revocation will occur no later than twenty-four (24) hours following such termination.

3. Intrusion Prevention. Abnormal utilizes reasonable measures designed to ensure that its infrastructure protections are consistent with industry standards in preventing unauthorized access to Abnormal networks, servers, and applications. Such measures include but are not limited to the implementation of intrusion prevention technologies, anti-malware services, and firewall rules.

4. Physical Access. Abnormal limits physical access to its office facilities using physical controls (e.g., coded badge access). Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that access to their data

centers and other areas where Customer Data is stored is limited to authorized individuals. Cloud hosting provider data centers and Abnormal office facilities leverage camera or video surveillance systems at critical internal and external entry points and are monitored by security Personnel.

5. Environmental Protection. Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that cloud hosting provider data centers implement and maintain appropriate and reasonable environmental controls for its data centers and other areas where Customer Data is stored, such as air temperature and humidity controls, and protections against power failures.

6. Backup, **Disaster Recovery, and Business Continuity**. Abnormal will: (a) back up its production file systems and databases according to a defined schedule and conduct regular testing of backups; and (b) maintain a disaster recovery plan for the production data center and maintain business continuity plans designed to manage and minimize the effects of disaster events or unplanned operational disruptions with a stated goal of resuming routine service within forty-eight (48) hours; and (c) conduct regular testing of the effectiveness of such plans.

7. Security Incident Response. For purposes of this Policy, any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data is a "**Security Incident**". Abnormal will: (a) take reasonable measures to implement and maintain logging and monitoring technologies designed to identify, alert, and analyze security events; and (b) maintain plans and procedures to be followed in the event of an actual or suspected Security Incident ("**Incident Response Plans**"). The Incident Response Plans require Abnormal to undertake a root cause analysis of any actual or suspected Security Incident and to document remediation measures.

8. Security Incident Notification. Abnormal will implement and follow procedures that are designed to detect and respond to Security Incidents and will notify Customer of any Security Incident affecting its Customer Data within forty-eight (48) hours of Abnormal becoming aware of the Security Incident, regardless of whether the Security Incident triggers any applicable breach notification law. Such notification will be executed using the contact information provided by Customer under the Records and Validation section of the Agreement.

Notice to a Customer will include: (a) a description of the nature of the Security Incident, including the categories and approximate number of Customer's data subjects and personal data records concerned; (b) the name of Abnormal's contact where more information can be obtained; (c) a description of the likely consequences of the Security Incident; (d) a description of the measures taken or proposed to address or mitigate the adverse effects of the Security Incident, to the extent within Abnormal's reasonable control.

9. Storage and Transmission Security. Abnormal will logically segregate Customer Data from all other Abnormal or third-party data. Abnormal will: (a) securely store Customer Data; (b) encrypt Customer Data during transmission using, at a minimum, Transport Layer Security (TLS) protocol version 1.2 or above; and (c) encrypt Customer Data at rest using, at a minimum, the Advanced Encryption Standard (AES) 256-bit encryption protocol. Abnormal will establish encryption key management processes that are designed to ensure the secure generation, storage, distribution, and destruction of encryption keys. Abnormal will not store Customer Data on any removable storage devices or other similar portable electronic media.

10. Data Retention and Secure Disposal. Abnormal will retain and securely dispose of Customer Data in accordance with the Agreement. During the Subscription Term, Customer may through the features of the Service access, return to itself or delete Customer Data. Following termination or expiration of the Agreement, Abnormal will delete all Customer Data from Abnormal's systems. Deletion will be in accordance with industry-standard secure deletion practices. Abnormal will issue a certificate of deletion upon Customer's written request. Notwithstanding the foregoing, Abnormal may retain Customer Data: (a) as required by applicable laws, or (b) in accordance with its standard backup or record retention policies, as governed by the Agreement.

11. Risk Identification and Assessment. Abnormal will implement and maintain a risk assessment program to help identify foreseeable internal and external risks to Abnormal's information resources and to Customer Data, and determine if existing controls, policies, and procedures are adequate.

12. Subprocessors. Abnormal will authorize third-party service providers to access or process Customer Data ("**Subprocessors**") only in accordance with the requirements and procedures specified in the Agreement, and specifically in the DPA. Prior to authorizing Subprocessors, Abnormal security Personnel will conduct a risk assessment of each Subprocessor to seek assurances of its data security practices (e.g., in the form of an independent third-party audit report such as the SOC 2 Type 2, ISO 27001, or a vendor security and risk evaluation). Abnormal enters into written agreements with its Subprocessors with security and data processing obligations substantially the same as those contained in this Policy.

13. Change and Configuration Management. Abnormal has implemented and will maintain processes for managing changes and updates to production systems, applications, and databases, including without limitation, processes for documenting, testing, and approval of changes into production, security patching, and authentication.

14. Release Management. Abnormal follows a continuous release process versus a standard release schedule and does not require a maintenance downtime window for the Service when pushing a new release. No Customer interaction is required to upgrade to the new version; the release is automatically applied to all Customers. Releases follow Abnormal's change management procedures that are designed to ensure that releases are tested and approved prior to push to production. Abnormal communicates release information using the notification functionality within the Service.

15. Training. Abnormal will undertake the following measures that are designed to ensure that Personnel who will have access to Customer Data are appropriately qualified and trained to handle Customer Data:

15.1. Information Security and Privacy Awareness Training. Upon hire and at minimum annually thereafter, Abnormal will require security and privacy awareness training to all Personnel who will process or have access to Customer Data. Abnormal security and privacy awareness training is designed to meet industry standards and will include, at a minimum, education on safeguarding against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, and social engineering mechanisms.

15.2. Secure Code Training. Abnormal will require annual training on secure coding principles and their application at minimum annually to all Personnel who develop or handle any Abnormal source code. Abnormal secure code training will cover topics such as: (a) the Open Web Application Security Project list of the 10 most critical security risks to web-based applications (OWASP Top 10); and (b) appropriate techniques for the remediation of the listed security vulnerabilities.

16. Background Checks. Abnormal Personnel will undergo a civil and criminal background check, to the extent permitted by applicable law.

17. Audit and Assessments. Abnormal has implemented and will maintain a Compliance Audit Program including assessments performed by an independent third-party ("**Auditor**") and defined Customer audit rights in accordance with the Agreement.

17.1 Independent Security Audit. Abnormal will engage an Auditor to certify compliance with the ISO 27001 standard, and conduct a SOC 2 Type 2 audit with a scoped audit period of a maximum 12 months to demonstrate its compliance with the security requirements of the Security Program. Abnormal's SOC 2 Type 2 audit covers the Trust Services Criteria of Security, Availability, Confidentiality, and Privacy. Abnormal will make available to Customer publicly available certificates and summary copies of its SOC 2 Type 2 audit report (each, an "**Audit Report**") on the Security Hub.

17.2 Customer Audits. Abnormal will make available the information necessary to demonstrate its compliance with the Security Program to support Customer in obtaining the information necessary to complete Customer's audits, reviews, risk assessments, and security-related questions of Abnormal as Customer's vendor. Please see the Security Hub for this information. For further details on Customer audit rights, please see your Data Processing Addendum (DPA).

17.3 Penetration Tests. At least once per twelve (12) month period, Abnormal will undertake a network penetration test by an independent third-party. Abnormal will make available to Customer an executive summary section of the penetration test report that pertains to the systems and operations that process, store, or transmit Customer Data. Abnormal will remediate all vulnerabilities that the penetration test identifies in accordance with the following remediation timelines:

Level	**Timeline**
Critical	15 days
High	30 days
Medium	60 days
Low	Reasonable timeframe based on nature and probability of exploitation

18. Artificial Intelligence Governance.

18.1. Abnormal uses industry standards to adopt, maintain, and adhere to policies and procedures related to the development and use of artificial intelligence ("**AI**") in the Service, including but not limited to the design, development, testing, evaluation, validation, verification, and deployment of AI.

18.2. AI used as a part of the Service is designed to: (i) be in compliance with applicable laws and regulations over the use of AI; (ii) be responsible and ethical in its use; (iii) minimize bias; (iv) minimize hallucinations; (v) introduce human involvement

where appropriate for corrective action; and (vi) not introduce any action or decision that impact the fundamental rights or safety of natural persons.

18.3. Abnormal will make available to Customer a summary, in plain language, at security.abnormalsecurity.com information about the use of AI in the Service and AI governance so that Customer may perform AI assessments.

All information exchanged between the Parties in the course of the activities described in all Sections above are deemed to be Abnormal Confidential Information.

EXHIBIT D

Abnormal Security Acceptable Use Policy

This Acceptable Use Policy (“AUP”) describes the prohibited uses of the Software as a Service offering (the "Service") provided by Abnormal Security Corporation (“Abnormal"). This AUP is in addition to any other terms and conditions under which Abnormal provides the Service to you. In addition to any other remedies available to Abnormal, if Abnormal determines in its sole discretion that you violate the AUP, we may suspend, limit, or terminate your use of the Service without prior notice or liability. This right applies, even if the breach is unintentional or unauthorized, if we believe that any such suspension, limitation, or termination is necessary to ensure compliance with laws, or to protect the rights, safety, privacy, security, or property (including the Service) of Abnormal or others.

Abnormal may modify this AUP at any time by posting an updated version of this document. Such updates will be effective upon posting. We therefore recommend that you visit the Abnormal website regularly to ensure that your activities conform to the most recent version. Your continued access to and use of the Service constitutes your agreement to be bound by such updates.

The prohibited uses listed below are not exhaustive. Prohibited uses and activities by you, the customer, your users or any third party include, without limitation:

- Violating any applicable laws or regulations (including without limitation data, privacy, and export control laws) or use the Service in a manner that gives rise to civil or criminal liability;
- Intentionally distributing malicious code, viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive manner;
- Infringing or misappropriating Abnormal’s or any third party’s intellectual property, proprietary or privacy rights;
- Reverse engineering, decompiling, or disassembling the Service or any software used in the provision of the Service;
- Using the Service or any Output or Anomaly Determinations to develop, train, or improve any AI or ML models (separate from authorized use of the Service under the Agreement);
- Representing any Output as being: approved or vetted by Abnormal; an original work or a wholly human-generated work;
- Use the Service or any Output to infringe any third-party rights;
- Using the Service for: (a) automated decision-making that has legal or similarly significant effects on individuals, unless it does so with adequate human review and in compliance with Laws; or (b) purposes or with effects that are discriminatory, harassing, harmful or unethical;
- Interrupting, or attempting to interrupt, violate, obtain unauthorized access to, disrupt, damage, overburden, breach, or compromise the operation or security of the Service or any networks or systems;
- Using the Service for any reason other than as intended by the parties.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

EXHIBIT E

ABNORMAL SECURITY CORPORATION SUPPORT AND SERVICE LEVEL AVAILABILITY POLICY

This Support and Service Level Availability Policy ("**Policy**") describes Abnormal Security Corporation's ("**Abnormal**") support offering ("**Support**") in connection with Customer-reported bugs, defects, or errors in the Service ("**Error(s)**"). Support shall be provided in accordance with the written subscription agreement under which Abnormal provides its Service as entered into by and between you ("**Customer**") and Abnormal ("**Agreement**"). Customer shall receive the level of Support set forth in this Policy or as designated in the applicable Order ("**Support Level**"). Abnormal may update this Policy from time to time, provided that any such update does not modify any provision of the Agreement except for this Policy. Any such updates will be posted to https://legal.abnormalsecurity.com/ or otherwise made available as set forth in the Agreement. Capitalized terms not defined in this Policy shall have the meanings given to them in the Agreement.

I. **Support**

1. **General Support Offering**. Abnormal shall provide English-speaking remote assistance to Customer Contacts (as defined below) for questions or issues arising from any Error, as further described in this Policy, including troubleshooting, diagnosis, and recommendations for potential workarounds for the duration of Customer's subscription to the applicable Service.

2. **Customer Contacts**. Customer shall inform Abnormal as to its approved contacts for Support, one of which must be designated as an account administrator (each, a "**Customer Contact**"). Customer is solely responsible for maintaining an accurate list of Customer Contacts with Abnormal, including names and contact information. Abnormal assumes no responsibility for Support Cases that cannot be addressed due to a lack of updated Customer Contact information.

3. **Submitting Support Cases.** Customer Contacts must use reasonable diligence to ensure a perceived Error is not an issue with Customer's own equipment, software, or internet connectivity prior to requesting Support. Customer Contacts may contact Support by submitting a Support request (each, a "**Support Case**") to: (a) the support portal located at https://support.abnormalsecurity.com (or such successor URL as may be designated by Abnormal) (such website, the "**Support Portal**") or (b) the web interface as described in the Documentation. If Customer Contacts cannot access the Support Portal they may open a Support Case by emailing support@abnormalsecurity.com or, in the event Customer Contacts cannot access the Support Portal or email, they may contact Abnormal Support by phone solely for purposes of having the Support Case submitted on their behalf. All Customer Contacts must be familiar with the Documentation and be reasonably trained in the use and functionality of the Service. Customer Contacts will assist Abnormal to resolve Support Cases by complying with the Customer obligations set forth in Table 1.

4. **Support Cases.** Each Support Case shall: (a) designate the Severity Level of the Error in accordance with the definitions in Table 1; (b) identify the Customer account that experienced the error; (c) include information sufficiently detailed to allow Abnormal to attempt to duplicate the Error (including any relevant error messages, but **not** export-controlled data, personal data (other than as required herein), sensitive data, other regulated data, or Customer Data); and (d) identify the Customer Contact most familiar with the issue. The Customer Contact shall also give Abnormal any other important Support Case information requested by Abnormal in a timely manner. Unless Customer expressly designates the Severity Level, the Support Case will default to Severity Level 4. If Customer Contacts submit Support Cases related to enhancement or feature requests, Abnormal shall treat those tickets as closed once the request has been forwarded internally.

Table 1: Error Severity Level Definitions and Initial Response Times			
Error Severity Level	**Description**	**Initial Response Time Target**	**Customer Responsibility**
Severity Level 1 (Urgent)	**An Error that causes a (a) service disruption or (b) degraded condition that renders the Service inoperable.**	**One (1) Hour**	**Commit appropriate resources to provide additional information as needed. Make reasonable efforts to apply solutions quickly.**
Severity Level 2 (High)	**An Error that (a) causes the Service to operate in a degraded condition with a high impact to key portions of the Service or (b) seriously impairs Customer's use of material function(s) of the Service and Customer cannot reasonably circumvent or avoid the Error without the expenditure of significant time or effort.**	**Two (2) Business Hours**	**Commit appropriate resources to be available to provide additional information as needed. Make reasonable efforts to apply solutions upon receipt.**
Severity Level 3 (Normal)	**An Error that has a medium-to-low impact on the Service. The Service is (a) running with limited functionality in one or more areas or (b) experiencing intermittent issues. Customer can access and use the material functionality of the Service.**	**Eight (8) Business Hours**	**Monitor and respond as necessary.**
Severity Level 4 (Low)	**How-to questions and Service issues with no Service degradation.**	**One (1) Business Day**	**Monitor and respond as necessary.**
RFE	**Requests for enhancements to the Service.**	**Two (2) Business Days**	**N/A**

5. **Other** Support and Training. Abnormal also offers various support and training resources such as documentation, FAQs and user guides available on the Abnormal Community.

6. **Error Response.** Abnormal Support will investigate Errors and assign the applicable Severity Level listed in Table 1. If Abnormal's Severity Level designation is different from that assigned by Customer, Abnormal will promptly notify Customer of such designation. If Customer notifies Abnormal of a reasonable basis for disagreeing with Abnormal's designated Severity Level, the parties each will make a good faith effort to discuss, escalate internally, and mutually agree on the appropriate Severity Level. Abnormal shall use commercially reasonable efforts to meet the Initial Response Time Target for the applicable Severity Level, as measured during the Support hours set forth in Table 2 below (with the total Business Hours in an in-region support day each a "Business Day").

Table 2: Support Hours			
Region	**North America**	**EMEA**	**Asia Pacific**
Severity 1	**24 x 7 x 365**	**24 x 7 x 365**	**24 x 7 x 365**
Severity 2-4	**6AM-6PM PT Mon-Fri**	**8AM-5PM GMT Mon-Fri**	**8AM-5PM AEDT Mon-Fri**
Exclusions	**U.S. Federal Holidays**	**United Kingdom Public and Bank Holidays**	**Australian National and Public Holidays**

II. **Service Level Agreement**

The Monthly Availability Percentage for the Service is ninety-nine and nine-tenths percent (99.9%) ("**Service Level**"). If the Service does not meet the Service Level in a given month ("**Service Level Failure**"), then as Customer's sole and exclusive remedy, Customer shall be eligible to receive the applicable number of Service level credits set forth in Table 3 below ("**Service Level Credits**"), credited towards extending Customer's Subscription Term at no charge, provided that Customer requests Service Level Credits within thirty (30) days from the time Customer becomes eligible to receive Service Level Credits under this Policy by filing a Support Case. Failure to comply with this notification requirement will forfeit Customer's right to receive

Service Level Credits. The aggregate maximum amount of Service Level Credits for a Service Level Failure will not exceed 15 days per month. Service Level Credits may not be exchanged for, or converted to, monetary amounts. Customer may request the Service Level attainment for the previous month by filing a Support Case.

Table 3: Service Level Credits	
Monthly Availability Percentage	**Service Level Credit**
< 99.9% - ≥ 98.0%	**3 Days**
< 98.0% - ≥ 95.0%	**7 Days**
< 95.0%	**15 Days**

Policy Exclusions

Abnormal will have no liability for any failure to meet the Service Level to the extent arising from: (a) Planned Maintenance or Emergency Maintenance; (b) third-party platforms and networks, Customer or User application, equipment, software or other third-party technology; (c) Customer or its User's use of the Service in violation of the Agreement or not in accordance with the Documentation; (d) force majeure events — i.e., any cause beyond such party's reasonable control, including but not limited to acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, public health emergencies (including pandemics and epidemics), acts or orders of government, acts of terrorism, or war; or (e) any access to the Service (or Service features) on a free, trial, beta or early access basis, or due to suspension, limitation, and/or termination of Customer's access or use of the Service in accordance with its Agreement.

Definitions:
"**Calendar Minutes**" is defined as the total number of minutes in a given calendar month.
"**Emergency Maintenance**" means circumstances where maintenance is necessary to prevent imminent harm to the Service, including critical security patching.
"**Monthly Availability Percentage**" is defined as the difference between Calendar Minutes and the Unavailable Minutes, divided by Calendar Minutes, and multiplied by one hundred (100).
"**Planned Maintenance**" means routine maintenance periods that continue for no more than four hours in any one instance, so long as Abnormal provides at least 48 hours prior notice (including by email) to Customer.
"**Unavailable**" means if Customer is unable to access the Service by means of a web browser and/or API as a result of failure(s) in the Service, as confirmed by Abnormal.
"**Unavailable Minutes**" is defined as the total accumulated minutes when the Service is Unavailable.