Attachment B

Cloudflare Terms and Conditions of Use

THE TERMS OF THE ADDENDUM, INCLUDING ITS ATTACHMENTS, AS MODIFIED, (THE "AGREEMENT") GOVERN THE ACCESS AND USE OF SERVICES MADE AVAILABLE BY CLOUDFLARE, INC. ("CLOUDFLARE"). A SUBSCRIBER ("CUSTOMER") MAY ONLY SUBSCRIBE TO THE SERVICES THROUGH CLOUDFLARE OR ITS APPROVED PARTNERS, SUCH AS A RESELLER, DISTRIBUTOR, MANAGED SERVICE PROVIDER, OR PLATFORM PROVIDER (EACH A "PARTNER"), AS AUTHORIZED BY CLOUDFLARE IN A WRITTEN AGREEMENT WITH SUCH PARTNER.

Definitions. The following definitions apply in these Terms:

1.1 "Customer Account Information" means the information Customer provides upon subscribing to the Services, audit logs, and Customer's account settings.

1.2 "Customer Content" means any files, software, scripts, multimedia images, graphics, audio, video, text, data, or other objects originating or transmitted from or processed by any Internet Properties owned, controlled or operated by Customer or uploaded by Customer through the Services, and routed to, passed through, processed and/or cached on or within, Cloudflare's network or otherwise transmitted or routed using the Services by Customer.

1.3 "Customer Data" means collectively, Customer Account Information, Customer Content and Customer Logs.

1.4 "Customer Logs" means any logs of End Users' and administrative users' interactions with Customer's Internet Properties and the Service that are made available to Customer via the Service dashboard or other online interface during the Term by Cloudflare.

1.5 "Documentation" means all printed and online user manuals and other technical materials relating to the Services made available to Customer by Cloudflare, as may be updated from time to time. Legal terms and conditions that are incorporated into the Documentation are no force or effect.

1.6 "End User" means a third-party visitor or user of Customer's Internet Properties and/or services delivered thereon and Customer's employees, agents or contractors who access or use the Services.

1.7 "Intellectual Property Rights" means any and all now known or hereafter existing worldwide: (a) rights associated with works of authorship, including copyrights, mask work rights, and moral rights; (b) trademark or service mark rights; (c) trade secret rights; (d) patents, patent rights, and industrial property rights; (e) layout design rights, design rights, and other proprietary rights of every kind and nature other than trade dress, and similar rights; and (f) all registrations, applications, renewals, extensions, or reissues of the foregoing.

1.8 "Internet Properties" means a root domain or website, including any subdomain thereof, or any internet connected application.

1.9 "Laws" means the applicable domestic, foreign local, state, federal, supranational, or international laws and regulations, including, without limitation, any data protection laws, regulations and treaties applicable to the respective Party ("Laws"). For the avoidance of doubt, the Parties understand and agree that, to the maximum extent permitted by Law, this Agreement shall be governed according to federal, state, and local laws and as otherwise set forth in Section 4(m) of the Addendum (GOVERNING LAWS, JURISDICTION, AND VENUE).

1.10 "Malicious Code" means viruses, worms, time bombs, Trojan horses, and other malicious code, files, scripts, software agents and programs.

1.11 "Network Data" means all models, observations, reports, analyses, statistics, databases, and other information created, compiled, analyzed, generated, or derived by Cloudflare from server, network or traffic data generated by Cloudflare in the course of providing the Service.

1.12 "Order Form" means Cloudflare's generated order form(s) and/or insertion orders for Services executed or approved by Partner for the Services to be made available to Customer.

1.13 "Services" means Cloudflare's cloud-based solutions, along with any software made available by Cloudflare in connection with such services, including software development kits and application programming interfaces.

1.14 "Subscription" means an annual or multi-year subscription to Services as reflected in an Order Form.

2. Terms Binding on Customer.

2.1 RESERVED.

2.2 Customer acknowledges that Cloudflare only provides Services to Customer as requested by Partner in Order Form(s) and that Partner is solely responsible to ensure Order Form(s) correctly reflect Customer's order with Partner. Customer therefore acknowledges and agrees that: (a) Customer only has the access and use rights set out in these Terms and the Order Form(s) regardless of any order or agreement with Partner; (b) any conditions in these Terms apply to Customer regardless of whether they are included in an agreement with Partner and (c) Cloudflare is not responsible for any discrepancy between Customer's order through the Partner and the Order Form(s).

3. Services; Restrictions.

3.1 Access Rights. Subject to Customer's compliance with the terms of the Agreement and the terms of Customer's agreement with Partner, Cloudflare will make the Services included in Customer's Subscription available for the duration of the Subscription for use and access by Customer and its administrative users solely for the Customer's internal business purposes, and solely in accordance with the terms of the Agreement and the Documentation.

3.2 Restrictions and Acceptable Use. Customer must not: (a) modify, copy, or create derivative works based on, the Service or Documentation; (b) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, or otherwise make the Service available to any third parties for use on any Internet Properties that are not owned and operated by Customer; (c) reverse-engineer the Service; (d) interfere with, or create an undue burden on the Service or Cloudflare's network in a manner that poses or has the potential to pose significant harm to Cloudflare's other customers or internal systems; (e) send or store infringing, obscene, threatening, or otherwise unlawful or tortious material, including material that violates privacy rights, through the Service; (f) use the Service in violation of any Laws; (g) send or store Malicious Code in connection with the Service; (h) probe, scan or test any vulnerability of the Services, including, without limitation, performing penetration, stress or load testing, including by introducing software or automated agents or scripts, other than those expressly permitted by the Agreement or Documentation or as explicitly set forth in the Order Form, without prior written consent from Cloudflare; (i) perform or publish any performance or benchmark tests or analyses relating to the Service, other than solely for Customer's internal use; or (j) cover or obscure any page or part of the Service via HTML/CSS, scripting, or any other means.

3.3 Credentials. Customer is responsible for maintaining the confidentiality of all usernames and passwords created by or assigned to Customer's administrative users ("**Credentials**") and may be responsible for all activities that occur under such Credentials. Customer agrees to notify Cloudflare promptly of any actual or suspected unauthorized use of any Credentials. Cloudflare reserves the right to terminate any Credentials that Cloudflare reasonably determines may have been accessed or used by an unauthorized third party and will provide immediate notice of such to Customer and promptly replace such Credential upon request. Credentials may not be shared or used by more than one individual but may be reassigned to a new individual if any individual with Credentials no longer needs access requiring Credentials. For its added security, Cloudflare strongly encourages Customer to enable two-factor authentication in conjunction with all Credentials. Upon termination or expiration of the Subscription, all Credentials associated with the Customer's administrative users will be deactivated and Customer will immediately discontinue use of the Services.

3.4 Support Services; SLA. Cloudflare will provide technical support for the Services during the Term at the level included in Customer's Subscription in accordance with Cloudflare's Enterprise Customer Support and Service Level Agreement attached to the Addendum as Attachment C ("**Enterprise Support SLA**"). If Cloudflare fails to meet the applicable service levels set forth in the Enterprise Support SLA (each such failure, a **"Service Failure"**), then as Customer's sole and exclusive remedy for any such Service Failure, Cloudflare will provide, at Customer's written request, Service Credits in accordance with the Enterprise Support SLA. Any Service Credits issued to Customer will be remitted to the Partner, and Partner will be solely responsible for providing such credits to Customer. If Customer subscribes to Services via a platform or managed service provider, no support services or service level agreements of any kind are included in these Terms and must be purchased from the Partner or via separate agreement.

3.5 Data Processing and Privacy. When and where applicable, the data processing addendum ("**DPA**") attached to the Addendum as Attachment D, applies to the processing of personal data on behalf of Customer. To the extent Cloudflare is the controller of personal data, Cloudflare's privacy policy set out at https://www.cloudflare.com/privacypolicy/ applies.

3.6 Supplemental Terms. Certain Services are subject to additional terms contained in the applicable Order Form.

4. Proprietary Rights.

4.1 Cloudflare Intellectual Property. Cloudflare reserves and retains all rights, title and interest in the Services, the Documentation, Network Data (including the right to use Network Data for purposes of providing, maintaining, developing, and improving its Services) and any of Cloudflare's proprietary technology, including, without limitation, any software, processes, scripts, algorithms, user interfaces, know-how, technologies, designs, and/or other tangible or intangible technical material or information that Cloudflare makes available to the Customer during the course of providing the Services, together with all updates thereto and all Intellectual Property Rights therein (collectively, "**Cloudflare Technology**") and Cloudflare or its licensors retain ownership in all Intellectual Property Rights related thereto. Cloudflare grants to Customer a limited right to use, reproduce, modify, and otherwise exploit the Network Data in connection with Customer's use of the Services, to the extent such Network Data are generally made available through the Services' dashboard or other online interface during the Subscription term. Cloudflare®, and any other product and service names and logos used or displayed in or on the Services are registered or unregistered trademarks of Cloudflare (collectively, "**Cloudflare Marks**"), and may not be used by Customer without Cloudflare's prior written consent. Customer must not attempt, now or in the future, to claim any rights in the Cloudflare Marks or use the Cloudflare Marks to disparage or misrepresent Cloudflare, or the Services.

4.2 Customer Intellectual Property. Customer reserves and retains all rights, title and interest in Customer Data and Customer feedback and Customer or its licensors retain ownership in all Intellectual Property Rights related thereto. Customer hereby grants Cloudflare a worldwide, non-exclusive, limited right of use (including to store, copy, transmit and display) Customer Data solely as permitted under the terms of the Agreement and as required to provide the Services, revocable in accordance with the terms of the Agreement. Customer hereby grants Cloudflare a non-exclusive, royalty-free, worldwide, transferable, irrevocable, sublicensable, perpetual license to use or incorporate into the Cloudflare Technology any Customer feedback. All Customer feedback is provided by Customer on an "AS IS" basis without warranty of any kind.

5. Customer Obligations; Use of Customer Data

5.1 Customer Obligations. Customer will: (a) be responsible for configuring the encryption for all Customer Data (excluding Customer Account Information) that it transmits through the Services; (b) take commercially reasonable efforts to prevent unauthorized access to, or use of, the Services; (c) be solely responsible for keeping and maintaining its own copies of Customer Data, except for Customer Account Information; (d) notify Cloudflare promptly in writing of any unauthorized access or use of the Services or Credentials; and (e) be solely responsible for Customer-devised or Customer-implemented rules or settings (and associated misconfigurations and outages) and actions taken by Customer that might result in denial of service, availability issues, or performance degradation. EXCEPT AS EXPRESSLY SET FORTH IN THE DOCUMENTATION, UNDER NO CIRCUMSTANCE SHALL CLOUDFLARE BE LIABLE FOR ANY DELETION OR DESTRUCTION OF CUSTOMER DATA THAT CUSTOMER DID NOT BACK UP. Customer must back up the Customer Data before submitting to Cloudflare.

5.2 The ordinary operation of the Services requires Customer Data to pass through Cloudflare's network. Cloudflare may monitor and inspect the traffic on the Cloudflare network, including any related logs as necessary to perform the Services and to derive and compile Network Data. To the extent Network Data includes any Personal Data, Cloudflare will handle such Personal Data in compliance with the Agreement and applicable data protection laws. Cloudflare may use and retain Customer Account Information for business purposes related to the terms of the Agreement and to the extent necessary to meet Cloudflare's legal compliance obligations (including, for audit and anti-fraud purposes).

6. Third-Party Products and Services; Beta Services

6.1 Third-Party Products and Services. Customer may access or use, at Customer's sole discretion, certain third-party products and services that interoperate with the Services including, but not limited to: third-party apps found on the Cloudflare Apps store located at www.cloudflare.com/apps/, third-party service integrations made available through the Cloudflare Service dashboard or Application Programing Interfaces (APIs), and third-party products or services that Customer authorizes to access Customer's Cloudflare account using OAuth or other Credentials (collectively, "**Third-Party Products**"). Each Third-Party Product is governed by the terms of service, end user license agreement, privacy policies, and/or any other applicable terms and policies of the third-party provider. Customer's access or use of Third-Party Products is solely between Customer and the applicable Third-Party Products provider. Cloudflare does not make any representations, warranties, or guarantees regarding the Third-Party Products or the providers thereof, including, but not limited to, the Third-Party Products' continued availability, security, and integrity. Third-Party Products are made available by Cloudflare on an "AS IS" and "AS AVAILABLE" basis, and Cloudflare may cease providing them in the Cloudflare Apps Store at any time without entitling Customer to any refund, credit, or other compensation. Unless otherwise specified in writing by Cloudflare, Cloudflare will not be directly or indirectly responsible or liable in any manner, for any harms, damages, loss, lost profits, special or consequential damages, or claims, arising out of or in connection with the installation of, use of, or reliance on the performance of any of the Third-Party Products.

6.2 Beta Services. Cloudflare may make non-production Services ("**Beta Services**") available to Customer upon Customer's request. All Beta Services will be clearly designated as Beta Services in any Order Form or the Service's dashboard. Beta Services are intended for testing purposes only and may be accessed by Customer at Customer's sole discretion. Cloudflare may, but is not obligated to, provide support for the Beta Services or correct any bugs, defects, or errors in the Beta Services. Regardless of whether Cloudflare provides technical support for the Beta Services, the SLA will not apply to the Beta Services unless specified otherwise in the applicable Order Form. Cloudflare may discontinue, suspend, or remove Beta Services (including any Customer Data stored as part of the Beta Services) or Customer's access thereto at any time in Cloudflare's sole discretion and has no obligation to make them generally available. Customer understands that any information regarding Beta Services is Cloudflare's Confidential Information and Customer agrees not to disclose such information unless a Beta Service becomes generally available, except as required by Law, and to only use such information in connection with Customer's use of the Beta Services. Notwithstanding Section 10.1, Cloudflare will have no liability for any harm or damage arising out of or in connection with any Beta Services, including any obligation or liability with respect to Customer Data. Any configurations or Customer Data entered into Beta Services, and any customizations made to Beta Services by or for Customer, may be permanently lost.

7. Warranties and Disclaimers.

7.1 Mutual Warranties. Each party warrants that it has the authority to enter into the Agreement and, in connection with its performance of the Agreement and/or its use of the Services, will comply with all Law including, Laws related to data privacy, international communications and the transmission of technical or personal data as defined in the DPA.

7.2 Limited Warranty. Cloudflare warrants during the Subscription term to Customer that the Services will materially conform to the Documentation under normal use and circumstances. If Customer or Partner notifies Cloudflare of a breach of the foregoing warranty, Cloudflare will, at its option, either: (a) correct the nonconformity in the Service; or (b) issue a credit or refund of a portion of the fees paid to Cloudflare by Partner for the Subscription for the nonconforming Services that fairly and reasonably reflects, the diminished value of the nonconforming Service. Partner is solely responsible for providing to Customer any credit or refund based on Cloudflare providing a corresponding credit or refund to Partner, and Customer's recourse for Partner's failure to pay such credit or refund is solely with Partner. A Service Failure does not constitute a breach of this Limited Warranty and is exclusively addressed by the Enterprise Support SLA. The foregoing constitutes Customer's sole and exclusive remedy for any breach of this limited warranty.

7.3 Additional Cloudflare Warranties. Cloudflare warrants that (i) during the initial term and each renewal term of a Subscription the functionality of the Services will not be materially degraded; and (ii) to the best of its knowledge, the Services do not contain, and Cloudflare will not knowingly introduce, any Malicious Code. Cloudflare may sunset, retire or replace any Service or feature thereof if applicable to all customers of the affected Service, provided the functionality of the Service will not be materially degraded during the then current term. Cloudflare warrants that it has implemented and will maintain a comprehensive written information security

program that includes administrative, physical, and technical safeguards to protect Customer Data as required by the terms of Exhibit A to the Addendum.

7.4 Customer Warranties. Customer represents that to the best of its knowledge, Customer Data does not contain, and Customer will not knowingly introduce, any Malicious Code into the Cloudflare network.

7.5 Disclaimer. EXCEPT FOR THE WARRANTIES SET FORTH IN THIS SECTION 7, CLOUDFLARE MAKES NO, AND HEREBY DISCLAIMS ALL, WARRANTIES, REPRESENTATIONS, OR CONDITIONS, WHETHER WRITTEN, ORAL, EXPRESS, IMPLIED OR STATUTORY, PAST OR PRESENT, OR FROM A COURSE OF DEALING OR USAGE OF TRADE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. CLOUDFLARE CANNOT AND DOES NOT WARRANT THAT ALL ERRORS CAN BE CORRECTED, OR THAT OPERATION OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. THE SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS. CLOUDFLARE IS NOT RESPONSIBLE FOR ANY FAILURES OR DAMAGES ARISING FROM SUCH PROBLEMS.

8. Limitation of Liability.

8.1 Types of Damages. TO THE EXTENT LEGALLY PERMITTED UNDER LAW, IN NO EVENT WILL CLOUDFLARE OR ITS SUPPLIERS BE LIABLE TO CUSTOMER OR TO ANY THIRD PARTY FOR ANY SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, ANY DAMAGES OR COSTS DUE TO LOSS OF PROFITS, DATA, USE, GOODWILL, PERSONAL OR PROPERTY DAMAGE, OR THE COST OF PROCURING SUBSTITUTE PRODUCTS OR SERVICES) RESULTING FROM OR IN CONNECTION WITH THE TERMS OR CUSTOMER'S USE, OR INABILITY TO USE THE SERVICES OR OTHER PRODUCTS OR SERVICES HEREUNDER, REGARDLESS OF THE CAUSE OF ACTION OR THE THEORY OF LIABILITY, WHETHER IN TORT, CONTRACT, STRICT LIABILITY OR OTHERWISE, AND EVEN IF CLOUDFLARE HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES.

8.2 Amount of Damages. RESERVED.

9. Informal Dispute Resolution. RESERVED.

10. Indemnification.

10.1 By Cloudflare. Cloudflare will defend, indemnify, and hold harmless the Customer and its officers, directors, employees, and agents from and against any and all damage, cost, liability and expenses (including court costs and reasonable attorneys' fees) incurred as a result of claims of third parties arising from or that are based upon an allegation that Customer's use of the Services infringes any United States Intellectual Property Right. If any portion of the Services becomes, or in Cloudflare's opinion is likely to become, the subject of a claim of infringement, Cloudflare may, at Cloudflare's option: (a) procure for Customer the right to continue using the affected Services; (b) replace the affected Services with non-infringing services which do not materially impair the functionality of the Services for Customer; (c) modify the affected Services so that they become non-infringing; or (d) terminate the Services and work with Partner to provide a pro rata refund of any fees already paid by Customer to cover the remainder of the Subscription term, and upon such termination, Customer will immediately cease all use of the affected Services. Notwithstanding the foregoing, Cloudflare will have no obligation under this Section or otherwise with respect to any infringement claim to the extent based upon: (w) any use of the Services not in accordance with these Terms or the Documentation; (x) any use of the Services in combination with third party products, equipment, software or content (including Customer Data) not supplied by Cloudflare; or (z) any modification of the Services by any person other than Cloudflare or its authorized agents. TO THE EXTENT PERMITTED BY LAW, THIS SUBSECTION SETS FORTH CLOUDFLARE'S SOLE AND EXCLUSIVE OBLIGATIONS, AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO CLAIMS OF INFRINGEMENT OR MISAPPROPRIATION OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

10.2 By Customer. Customer understands and acknowledges that it is solely responsibility for the risks associated with its activities and contents on its Internet Properties or any misuse of the Services and that Cloudflare should not be held responsible for such risks. Therefore, to the extent permitted by applicable Law, Customer will defend, indemnify and hold harmless Cloudflare and its affiliates, licensors, suppliers, officers,

directors, employees and agents from and against any and all damage, cost, liability and expenses (including court costs and reasonable attorneys' fees) incurred as a result of claims of third parties arising from or that are based upon: (a) Customer's use of the Services in a manner not permitted by these Terms or the Documentation; (b) Customer Data or Customer's Internet Properties (including without limitation any activities or aspects thereof or commerce conducted thereon); or (c) Customer's non-compliance with Law.

10.3 Procedure. The indemnifying party's obligations as set forth above are expressly conditioned upon each of the following: (a) the indemnified party will promptly notify the indemnifying party in writing of any threatened or actual claim or suit; *provided*, that failure to provide such prompt notice will not release the indemnifying party from its indemnity obligations except to the extent it is materially prejudiced thereby; (b) the indemnifying party will have sole control of the defense or settlement of any claim or suit, except as provided in Section 3(e) of the Addendum; (c) the indemnified party will cooperate with the indemnifying party (at the indemnifying party's expense) to facilitate the settlement or defense of any claim or suit; and (d) the indemnifying party will not settle any claim or suit in a manner which results in an admission of liability by the indemnified party, without the indemnified party's prior written consent.

11. Term and Termination

11.1 The right to use and access the Services under the Agreement automatically terminates at the end of the Subscription term. Cloudflare may suspend or terminate any Subscription to the Services if Customer commits a material breach of the Agreement and, if curable, fails to cure such breach within thirty (30) days following receipt of notice of the breach from Cloudflare, or if instructed by Partner (with a written notice to Customer) to do so subject to the agreement between Customer and Partner.

11.2 When a Subscription terminates or expires, all rights and licenses granted to Customer automatically terminate and Customer must immediately cease use of the Services and return or destroy all copies of any software.

11.3 Except as otherwise agreed by Cloudflare in writing, no refunds or credits will be provided by Cloudflare, and Customer's sole recourse for any refund is against Partner.

12. General.

12.1 Compliance with Laws. Customer shall comply with all applicable Laws, and Customer is solely responsible for determining whether use of the Services will satisfy Customer's individual compliance obligations.

12.2 Assignment. RESERVED.

12.3 Confidential Information. RESERVED.

12.4 Force Majeure. RESERVED.

12.5 Notices. RESERVED.

12.6 Government Restrictions. If Customer is an agency, department or entity of the United States Government ("**Government**"), Customer understands and agrees, that (a) Customer's rights to use, reproduce, release, modify or disclose the Cloudflare Technology, or any part thereof, is restricted in accordance with Federal Acquisition Regulation ("**FAR**") 12.212 for civilian agencies and Defense Federal Acquisition Regulation Supplement ("**DFARS**") 227.7202 for military agencies, (b) the Cloudflare Technology consists of "commercial computer software" and "commercial computer software documentation," respectively, as defined in FAR Section 12.212 and DFARS Section 227.7202, or their successor provisions, as applicable and (c) use of the Cloudflare Technology by any Government agency, department or other agency of the Government is further restricted as set forth in these Terms.

12.7 Amendment. RESERVED.

12.8 Miscellaneous. The Parties are independent contractors, and neither Party is an agent, partner, or employee of the other Party. If any provision of the Agreement is deemed illegal or unenforceable by a court of competent jurisdiction, such provisions shall be limited or eliminated to the minimum extent necessary so that the Agreement shall otherwise remain in full force and effect. Headings are for convenience only and do not impact the construction of these Terms and "including" means "including but not limited to." Each Party participated equally in the preparation of the Agreement, and no ambiguity shall be resolved against any one

Party. Unless otherwise stated herein, all remedies are cumulative and not to the exclusion of any other rights and remedies available at law or in equity. The Parties acknowledge that any actual or threatened breach of Section 3.2 may constitute immediate, irreparable harm to the non-breaching Party, for which monetary damages may be an inadequate remedy, and that injunctive relief may be an appropriate remedy for such breach. To the extent permitted by Law, if any legal action is brought to enforce these Terms, the prevailing Party will be entitled to receive its attorneys' fees, court costs, and other collection expenses from the non-prevailing Party, in addition to any other relief the prevailing Party may receive. Any provision of the Agreement that explicitly or by its nature contemplates performance or observance after termination or expiration of the Agreement, shall so survive and continue in full force and effect.

END OF TERMS

State of North Carolina
Addendum
To the
Cloudflare's Agreement

Certain terms and conditions are required by applicable North Carolina law and regulation and are set forth below. Such terms supersede all conflicting terms in the **Cloudflare Terms and Conditions of Use (Attachment B), Cloudflare's Enterprise Customer Support and Service Level Agreement ("Enterprise Support SLA") (Attachment C), Cloudflare's Data Processing Addendum ("DPA") (Attachment D),** (collectively, Cloudflare's Agreement) from the date of execution set forth below. This Addendum together with Cloudflare's Agreement will be collectively referred to as the "Agreement."

The State acknowledges that Cloudflare's Agreement may include terms and conditions, hyperlinks, or similar references to additional license agreements, and that such additional license agreements address the proprietary and intellectual property rights of third parties for software or software services owned by parties other than Cloudflare (Third Party(ies)). The Agency further acknowledges that the proprietary and intellectual property rights of the Third Party are subject to a software license agreement. The Reseller shall provide the Agency with copies of all documentation and warranties for the Third-Party software and related services offered.

1) Cloudflare's Agreement is modified by this Addendum, and therefore, conflicts arising among the terms of the Cloudflare's Agreement and the terms of this Addendum shall be resolved by the following order of precedence:

   a) This Addendum
   b) Cloudflare's Agreement (Attachment B)
   c) Terms and other documents incorporated by reference in the Cloudflare's Agreement

2) To the extent required by Law, the State shall not be obligated under Cloudflare's Agreement, or other agreements, to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, legal fees, termination costs, costs of audits, or other similar costs.

3) General Modifications to Cloudflare's Agreement:

   a) Cloudflare's Agreement (Attachments B through D) are modified as follows: deletions are represented by strikethroughs (~~deletion~~), and insertions are represented by underlines (<u>insertion</u>). Attachments B through G, as modified, are attached hereto and are hereby incorporated herein.

   b) Reserved..

   c) Clickwrap / universal license by use or installation: Notwithstanding terms of the Cloudflare's Agreement conditioning the license grant or right of use upon acceptance of terms when downloading, installing, using, etc. the software (e.g., by using the software, you accept and agree to the terms and conditions of this agreement), such conditions shall not bind the State or its agencies, and such conditions shall be superseded by this Addendum to the Cloudflare's Agreement.

   d) Notwithstanding any payment terms in Cloudflare's Agreement, the State's payment obligations in its contracts with Resellers, if applicable, shall supersede the payment terms in Cloudflare's Agreement, and the State shall have no invoicing payment obligation to Cloudflare pursuant to the payment terms in Cloudflare's Agreement.

e) IP Indemnity – notwithstanding the Cloudflare's rights to defend its IP and its obligations to indemnify the State, the State shall have the right to participate in any litigation, alternative dispute resolution and settlement of such claims to the extent the State seeks to assert any immunities or defenses applicable to the State as a sovereign government.

f) To the extent required by Law, neither Party to this Addendum is entitled to obtain judgment from the other party for attorney fees it has incurred in any litigation between the Parties or in defense of any claim asserted by a third party. Either party may seek such equitable relief, reasonable costs and fees as permitted by applicable law.

g) Notwithstanding any term in the Cloudflare's Agreement prohibiting assignment or transfer of the agreement, transfers authorized by N.C.G.S. § 143A-6 are not prohibited or limited.

h) Notwithstanding any merger clauses in Cloudflare's Agreement, this Addendum shall be read together with the Cloudflare's Agreement as the Agreement of the Parties.

i) Vendor will comply with data localization (or offshoring requirements) designated by the State (e.g., Cloudflare for Government FedRamp services), provided and to the extent that: (a) such geographical localization functionality is available to the Services purchased by Customer and expressly set forth in such Documentation; and (b) such geographical localization functionality is properly activated by Customer in the Cloudflare Dashboard.

4) Certain terms and conditions are required by applicable North Carolina law and regulation and are set forth below. Such terms supersede all conflicting terms in Cloudflare's Agreement from the date of execution set forth below. State Terms and Conditions:

a) By executing this Addendum, the undersigned Vendor certifies that: Cloudflare's Agreement and this Addendum are entered without collusion (N.C.G.S. § 143B-1354; False certification is a Class I felony), that none of its officers, directors, or owners of an unincorporated business entity has been convicted of any violations of Chapter 78A of the General Statutes, the Securities Act of 1933, or the Securities Exchange Act of 1934 (N.C.G.S. § 143-59.2), and that it is not an ineligible Vendor as set forth in N.C.G.S. § 143-59.1. Furthermore, by executing this Addendum, the undersigned certifies to the best of Cloudflare's knowledge and belief that it and its principals are not presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from covered transactions by any Federal or State department or agency.

b) VENDOR UTILIZATION OF WORKERS OUTSIDE U.S.

In accordance with N.C.G.S. § 143B-1361(b), Cloudflare must identify the manner in which it intends to utilize resources or workers located outside the U.S. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such offer. Cloudflare shall provide the following for any offer or actual utilization or contract performance:

The location of work performed under a state contract by Cloudflare, any subcontractors, employees, or other persons performing the contract and whether any of this work will be performed outside the United States.

The corporate structure and location of corporate employees and activities of Cloudflare, its affiliates or any other subcontractors.

Notice of the relocation of Cloudflare, employees of Cloudflare, subcontractors of Cloudflare, or other persons performing Services under a state contract outside of the United States.

Any Vendor or subcontractor providing call or contact center Services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center Services are being provided.

Will any work under this contract be performed outside the United States?

☐ YES ☐ NO

If yes, please provide the location(s) outside of the United States: Cloudflare provides customer support and Sub-processor operations pursuant to the information and locations provided in the DPA.

For the avoidance of doubt, the State agrees that Cloudflare has satisfied all of the above information requests as of the date of signature of this Agreement, and that any new requests for such information may be provided by Cloudflare upon written request of the State.

---

c) E-VERIFY. Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

d) EXCLUSIVE REMEDIES AND LIMITATION OF LIABILITY

For purposes of the exclusive remedies and limitations of liability set forth herein, Vendor shall be deemed to include the Vendor and its employees, agents, representatives, subcontractors, and suppliers and damages shall be deemed to refer collectively to all injuries, damages, losses, liabilities, expenses or costs incurred.

Where Services are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Services and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Services.

The Vendor's liability for damages to the State arising under the contract shall be limited to two times the annual value of the Contract. Annual value is defined as the total cost of goods, software and services procured by the State from one or more of Cloudflare's Resellers pursuant to the state's contract. The existence of one or more claims under the terms will not increase either Party's liability.

The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to, Service Level Agreement or Deliverable/Product Warranty compliance, or to claims for injury to persons or damage to tangible personal property, by Vendor's gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. § 1B-1 *et seq*., the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Agreement. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Agreement are intended to provide the sole and exclusive remedies available to the State under the Agreement for Cloudflare's failure to comply with the requirements stated therein.

For delays in the delivery or successful Product or Software installation, whichever is applicable, Cloudflare shall have no liability unless the delivery or successful installation date is delayed by more than thirty (30) days by causes not attributable either to the State or to Force Majeure conditions, in which case the State shall have the right, as its remedies:

i) To recover direct costs including replacement Products, if any, attributable to Cloudflare's delay, and

ii) To cancel the order without incurring cancellation charges.

Cloudflare shall have no liability unless the default in delivery of Services is occasioned by causes not attributable either to the State or to Force Majeure conditions.

e) TRANSPORTATION: Transportation charges for any software or other Deliverable shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order. The Parties agree and understand that transportation charges shall not apply for this Agreement unless expressly set forth in an Order Form.

f) TRAVEL EXPENSES: Reserved. (See NCDIT Terms and Conditions (SaaS) (Attachment A), Section # 12).

g) PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES: Cloudflare warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any contract or award issued by the State. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding Agreements. Violations of this provision may result in debarment of the Vendor(s) as permitted by 9 NCAC 06B.1206, or other provision of law.

h) AVAILABILITY OF FUNDS: Any and all payments by the State are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the Agency for the purposes set forth in this Agreement. If this Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the Agency's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of this Agreement extends into fiscal years subsequent to that in which it is approved such continuation of the Agreement is expressly contingent upon the appropriation, allocation, and availability of funds by the N.C. Legislature for the purposes set forth in the Agreement. If funds to effect payment are not available, the Agency will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to take back any affected Products and software not yet delivered under this Agreement, terminate any Services supplied to the Agency under this Agreement, and relieve the Agency of any further obligation thereof. The State shall remit payment for Services accepted prior to the date of the aforesaid notice in conformance with the payment terms.

i) ACCESS TO PERSONS AND RECORDS: Pursuant to N.C.G.S. § 147-64.7, the Agency, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of Cloudflare insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of this Agreement or to costs charged to this Agreement. Cloudflare shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of this

Agreement. Additional audit or reporting requirements may be required by any Agency, if in the Agency's opinion, such requirement is imposed by federal or state law or regulation.

j) CONFIDENTIALITY: In accordance with N.C.G.S. § 143B-1350(e) and 143B-1375, and 09 NCAC 06B.0103 and 06B.1001, the State may maintain the confidentiality of certain types of information described in the NC Public Records Act: N.C.G.S. § 132-1 *et seq*. Such information may include trade secrets defined by N.C.G.S. § 66-152 and other information exempted from the Public Records Act pursuant to N.C.G.S. § 132-1.2. Materials must be identified as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "CONFIDENTIAL". By so marking any page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State may serve as custodian of Cloudflare's confidential information and not as an arbiter of claims against Cloudflare's assertion of confidentiality. If an action is brought pursuant to N.C.G.S. § 132-9 to compel the State to disclose information marked confidential, Cloudflare agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). To the extent required by Law, Cloudflare agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify Cloudflare in writing of any action seeking to compel the disclosure of Cloudflare's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. To the extent required by Law, the State shall have no liability to Cloudflare with respect to the disclosure of Cloudflare's confidential information ordered by a court of competent jurisdiction pursuant to N.C.G.S. § 132-9 or other applicable law.

   i) The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC § 6103 and IRS Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC § 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the N.C. Department of Information Technology or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.

   ii) Cloudflare shall protect the confidentiality of all information, data, instruments, studies, reports, records and other materials provided to it by the Agency or maintained or created in accordance with this Agreement. No such information, data, instruments, studies, reports, records and other materials in the possession of Cloudflare shall be disclosed in any form without the prior written consent of the State Agency. Cloudflare will have written policies governing access to and duplication and dissemination of all such information, data, instruments, studies, reports, records and other materials.

k) ASSIGNMENT: Cloudflare may not assign this Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Any assignee shall affirm this Agreement accepting the terms and conditions and duties as previously agreed, and that Cloudflare shall affirm that the assignee is fully capable of performing all obligations of Cloudflarer under this Agreement. An assignment may be made, if at all, in writing by

Cloudflare, the Assignee and the State setting forth the foregoing obligation of Cloudflare and Assignee.

l) TERMINATION: Any notice or termination made under the Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.

i) The Parties may mutually terminate the Agreement by written agreement at any time.

ii) Termination for Cause: In the event any goods, Services, or service furnished by Cloudflare during performance fails to conform to any material specification or requirement of the Agreement, and the failure is not cured within the specified time after providing written notice thereof to Cloudflare, the State may cancel the articles or Services. Where such remedy is expressly required by Law, the State may procure such services from other sources; holding Cloudflare liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraph 4) d), entitled "Exclusive Remedies and Limitation of Liability." The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Agreement. Where expressly required by Law, Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of this Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.

iii) Termination For Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to Cloudflare and Reseller. Cloudflare shall be entitled to sums due via the Reseller, if applicable, as compensation for Deliverables and Services in conformance with the Agreement. Upon such termination for convenience, the State will pay to Vendor any and all fee amounts set forth in the active Order Forms, provided that payment of such amount will constitute the State's entire liability and Vendors sole remedy for such termination.

m) GOVERNING LAWS, JURISDICTION, AND VENUE: This Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina. The place of this Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Cloudflare agrees and submits, solely for matters relating to this Agreement, to the jurisdiction of the courts of the State of North Carolina and stipulates that Wake County shall be the proper venue for all matters. Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern the Agreement. To the extent the Contract entails both the supply of "goods" and "Services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such Services as "goods" would result in a clearly unreasonable interpretation.

n) ELECTRONIC PROCUREMENT: Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third-party agent shall serve as the Supplier Manager for this E-Procurement Service. Cloudflare shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract.

The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Service. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of contract, and the payment for goods delivered.

Cloudflare agrees at all times to maintain the confidentiality of its username and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Cloudflare shall be responsible for all activity and all charges for such employees. Cloudflare agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through Cloudflare's account, Cloudflare shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Cloudflare shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

o) Solutions Not Hosted on State Infrastructure

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

(a) Vendors shall provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission. This report is located at the following website: https://it.nc.gov/documents/vendor-readiness-assessment-report

(b) Upon request, Vendors shall provide a current independent 3rd party assessment report in accordance with the following subparagraphs (i)-(iii) prior to contract award. However, Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(iii) at the time of offer submission.

(i) Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).

(ii) A Vendor that cannot provide a preferred independent 3rd party assessment report as described above may submit an alternative assessment, such as a SOC 2 Type 1 assessment report. The Vendor shall provide an explanation for submitting the alternative assessment report. If awarded this contract, a Vendor who submits an alternative assessment report shall submit one of the preferred assessment reports no later than 365 days of the Effective Date of the contract. Timely submission of this preferred assessment report shall be a material requirement of the contract.

(iii) An IaaS vendor cannot provide a certification or assessment report for a SaaS provider UNLESS permitted by the terms of a written agreement between the two

vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.

(c) Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to executive summary penetration test reports. The awarded Vendor shall provide such additional security documentation upon request by the State during the term of the contract.

5. Additional NC Department of Information Technology Terms and Conditions for a Software - as-a-Service (SaaS) application are attached hereto as Attachment A and hereby incorporated herein.

Signatures follow on next page

Executed by authorized officials as of the day and date indicated below.

North Carolina Department of Information Technology	**Cloudflare, Inc.**
By:	By: A. Halsey Bertenthal
Name: Teena Piccione	Name: Halsey Bertenthal
Title: Secretary and State CIO	Title: Head of Commercial Legal
Date: 03/27/2025	Date: Mar 26, 2025

ATTACHMENT A
NC DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS
SOFTWARE-AS-A-SERVICE (SaaS)

1) DEFINITIONS:

a) "Data" includes information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

b) "Deliverable/Product Warranties" shall mean and include the warranties provided for products or deliverables licensed to the State as included in Paragraph 7) c) of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's Agreements or Support Agreements. The Parties understand and agree that "deliverables" and "products" are not applicable to this Agreement, and any such defined term used herein is in reference to the Vendor "Services" as defined in this Agreement.

c) "Services" shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation, including, without limitation, providing web browser access by authorized users to certain Vendor online software applications identified herein, and to related services, such as Vendor hosted Computer storage, databases, Support, documentation, and other functionalities, all as a Software as a Service ("SaaS") solution.

d) "State" shall mean the State of North Carolina, the NC Department of Information Technology (NCDIT) as an agency, or the agency identified in this solicitation as the Purchasing Agency and Award Authority.

e) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, other support Services as provided by the Vendor for SaaS tenants receiving similar SaaS Services.

2) ACCESS AND USE OF SAAS SERVICES:

a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so- called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et seq*.

b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.

c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor's SaaS tenants for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.

d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.

e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.

f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the security provisions referenced herein can still be complied with. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.

g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.

h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling, if applicable.

i) Intentionally omitted.

3) WARRANTY OF NON-INFRINGEMENT; REMEDIES.

a) Vendor warrants to the best of its knowledge that:

i) The Services do not infringe any intellectual property rights of any third party; and
ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.

b) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, trademark or a trade secret in the United States, the Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become non-infringing. If neither of these options can reasonably be taken in Vendor's judgment, or if further use shall be prevented by injunction, the Vendor agrees to cease provision of any affected Services and refund any sums the State has paid Vendor for unused services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from the Vendor under this Agreement impractical, the State shall then have the option of terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.

c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services supplied by the Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following:
i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.

d) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation results from the State's material alteration of any Vendor-branded Services, from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party, or any other exception expressly set forth in this Agreement.

4) ACCESS AVAILABILITY; REMEDIES:

a) The Vendor warrants that the Services will be in good working order and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services' functions will meet all the State's requirements, unless developed as Customized Services.

b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State.

c) Intentionally omitted.

5) EXCLUSIONS:

a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.

b) The warranties provided in Paragraphs 3 and 4 above do not cover repairs for damages, malfunctions or service failures substantially caused by:

i) Actions of non-Vendor personnel;
ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
iii) Force Majeure conditions set forth hereinbelow.
iv) The State's sole misuse of, or its own inability to use, the Services.

6) **PERFORMANCE REVIEW AND ACCOUNTABILITY.** Intentionally omitted.

7) **LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:** Reserved. (See Addendum 4) d).)

8) **VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY**:
   a) If Vendor personnel enters the States premises, Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
   b) Intentionally omitted.
   c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

9) **MODIFICATION OF SERVICES:** If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.

10) **TRANSITION PERIOD:**
   a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement by the State, Vendor shall make available for export the State, upon written request, all applicable Data ("Transition Period").
   b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
   c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
   d) Intentionally omitted.
   e) Upon termination, and unless otherwise stated in an SLA, and after making available the State Data to the State as indicated above in this section, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control. Upon request, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
   f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.

11) **TRANSPORTATION:** Reserved. (See Addendum 4) e).)

12) **TRAVEL EXPENSES:** **All travel expenses should be included in Vendor's proposed costs. Separately stated travel expenses will not be reimbursed.** In the event that the Vendor may be eligible to be reimbursed for travel expenses specifically agreed to in writing and arising under the performance of this Agreement, reimbursement will be at the out-of-state rates set forth in G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest

available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under this Agreement.

13) PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES: Reserved. (See Addendum 4) g).)

14) AVAILABILITY OF FUNDS: Reserved. (See Addendum 4) h).)

15) PAYMENT TERMS:

a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off if required by law and as permitted in Chapter 105A-1 *et seq*. of the N.C. General Statutes and applicable Administrative Rules. Payment terms in any applicable Order Form shall supersede the payment terms included in this Section 15.

b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:

   i) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or

   ii) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,

   iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.

c) For any third-party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State. The Parties understand and agree that this will not be applicable to the Services unless set forth expressly in an Order Form.

d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the date of receipt of the invoice, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency.

e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services

identified or associated with such invoices. The Parties understand and agree that retainages and this subsection shall not be applicable to the Services unless expressly set forth in an Order Form.

16) ACCEPTANCE CRITERIA:

a) Initial acceptance testing is required for all Vendor supplied Services before going live, unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications and Vendor's technical representations. Acceptance of Services may be controlled by additional written terms as agreed by the parties.

b) After initial acceptance of Services, the State shall have the obligation to notify Vendor, in writing and within ten (10) days following provision of any Deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a Deliverable is unacceptable. Acceptance by the State of any Vendor re-performance or correction shall not be unreasonably withheld but may be conditioned or delayed as required for confirmation by the State that the issue(s) in the notice have been successfully corrected.

c) The Parties understand and agree that the Services have already been accepted, and acceptance of the Services and this Section 16 shall not be applicable except as expressly set forth in any such Order Form.

17) CONFIDENTIALITY: Reserved. (See Addendum 4) j).)

18) SECURITY OF STATE DATA:

a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials. For the avoidance of doubt, the Parties understand and agree that the data rights and responsibilities set forth herein are to be construed in connection with (and not supersede) the data rights and responsibilities set forth in the Cloudflare Terms and Conditions of Use.

b) Intentionally omitted.

c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (https://it.nc.gov/document/statewide-data-classification-and-handling-policy) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of

data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within 48 hours of confirmation as required.

d) The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. To the extent possible, the Vendor will allow periodic back-up of relevant State Data by the State to the State's infrastructure or as may be provided by law.

e) The Vendor shall confirm to the State:
   i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement.
   ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
   iii) That the Services will comply with the following:
      (1) Any NCDIT security policy regarding Cloud Computing, and the NCDIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
         (a) The Vendor shall encrypt all non-public data in transit over public networks regardless of the transit mechanism.
         (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS 140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection.
      (2) Privacy provisions of the Federal Privacy Act of 1974.
      (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. §§ 75- 65 and -66);
      (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
      (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), and the Health Insurance Portability and Accountability Act (HIPAA);
      (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.

f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60 et seq.) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.

g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation/mitigation plan to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State may notify the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of its own remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under

the circumstances, including any applicable Charges for the same.

i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data.

j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.

k) Intentionally omitted.

l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.

m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:

   (1) The scale and quantity of the State Data loss;
   (2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
   (3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
   (4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

   Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (only if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.

n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

o) Secure Data Disposal. When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State upon written request.

19) ACCESS TO PERSONS AND RECORDS: Reserved. (See Addendum 4) i).)

20) **ASSIGNMENT:** Reserved. (See Addendum 4) k).)

21) **NOTICES:** Any notices required under this Agreement should be delivered to the Agreement Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier, facsimile or by hand. If the latest e-mail address provided to Partner by the State is not valid, or for any reason is not capable of delivering any notice required by these Terms, the State acknowledges and agrees that Vendor's or Partner's dispatch of an e-mail to such address will nonetheless constitute effective notice. Any notice provided to be provided to Vendor pursuant to these Terms should also be sent to the Partner.

22) **TITLES AND HEADINGS**: Titles and Headings in this Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

23) **AMENDMENT:** This Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor.

24) **TAXES**: The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of this Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

25) **GOVERNING LAWS, JURISDICTION, AND VENUE:** Reserved. (See Addendum 4) m).)

26) **DEFAULT**: Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.
   a) Intentionally omitted.
   b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such Vendor failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure. Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.

27) **FORCE MAJEURE:** Except as provided for herein, neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

28) **COMPLIANCE WITH LAWS:** The Parties shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and the provision of Services hereunder, including those of federal, state, and local agencies having jurisdiction and/or authority.

29) **TERMINATION:** Reserved. (See Addendum 4(l))

30) **DISPUTE RESOLUTION**: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the State shall be submitted in writing to the Vendor's Agreement Administrator for decision. The Parties shall negotiate in good faith and use all

reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under this Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under this Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

31) **SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of this Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of this Agreement shall remain in full force and effect. All promises, requirements, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

32) **FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:** The Parties agree that the State shall be entitled to any and all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. § 365(n), and any amendments thereto.

33) **ELECTRONIC PROCUREMENT**: Reserved.

ATTACHMENT C

Cloudflare Enterprise Customer Support and Service Level Agreement

Policy date: April 27, 2021

Capitalized terms not defined in this Cloudflare Enterprise Customer Support and Service Level Agreement ("**Terms**") have the meanings set forth in the Enterprise Subscription Agreement, between Cloudflare and Customer.

1. DEFINITIONS

1.1. **"Affected Customer Ratio"** is calculated as follows:

$$\text{Affected Customer Ratio} = \frac{\text{Unique Users as Measured by IP Address Affected by the Downtime Incident}}{\text{Total Unique Users as Measured by IP Address}}$$

1.2. **"Claim"** means a claim submitted by Customer to Cloudflare pursuant to these Terms.

1.3. **"Customer Planned Downtime"** means downtime in minutes expressly specified to Cloudflare by Customer, including, but not limited to, any time for which Customer has requested that Service access be suspended from their environment.

1.4. **"Incident"** means any set of circumstances resulting in an observable or reproduceable degradation of the Service.

1.5. **"Issue"** means any set of circumstances resulting in a failure to meet a Service Level.

1.6. **"Outage Period"** is the number of downtime minutes resulting from an Unscheduled Service Outage.

1.7. **"P1 Issue"** means any Issue in which the Service is significantly impaired and unavailable from multiple Internet Service Providers (ISPs) (e.g., a situation where one or more of Customer's websites are inaccessible to End Users in multiple geographies).

1.8. **"P2 Issue"** means any Issue in which Customer experiences a repeated inability to use the Service from a single ISP (e.g., a localized denial of service issue that is limited to a single website or even a single server).

1.9. **"P3 Issue"** means any non-urgent Issue that, whilst potentially Service impacting, does not prevent Customer's use of the Service in any material way (e.g., minor bugs or reports of unexpected behavior).

1.10. **"P4 Issue"** means any general question related to Cloudflare's products or services. For example, purely informational requests, reports, usage questions, clarifications regarding documentation, or any feature enhancement suggestions.

1.11. **"Scheduled Availability"** means the total number of minutes in a given month, minus any Customer Planned Downtime.

1.12. **"Service Levels"** means the service level commitments set forth in Section 2 of these Terms, and any other standards that Cloudflare chooses to adhere to and by which it measures the level of service provided to Customer.

1.13. **"Unscheduled Service Outage"** means an interruption to the Service that was not previously communicated to Customer, and that results in Customer's websites being unavailable to its own End Users. Unscheduled Service Outages exclude any: (i) Customer Planned

Downtime; and/or (ii) any downtime caused by a Service Level Agreement (SLA) exclusion listed in Section 8.1 below.

2. SERVICE LEVEL COMMITMENT

2.1. **Measurable Performance Enhancement**. The Service will serve Customer Content measurably faster than Customer's websites would serve Customer Content without use of the Service.

2.2. **100% Uptime**. The Service will serve Customer Content globally 100% of the time.

2.3. **Penalties**. If the Service fails to meet the above service level commitments, Customer will receive a credit from Cloudflare as set-forth in **Section 9** of these Terms (the **"Service Credit"**).

3. ACCESS TO SUPPORT

3.1. Customer will utilize Cloudflare's online account interface to manage and configure the Service.

3.2. Cloudflare will provide Customer with access to an online customer support center where Customer may: (i) open a Claim; (ii) send Cloudflare information to aid in the resolution of any Issues with the Service; (iii) check on the status of open Claims; (iv) track any correspondence between Customer and Cloudflare support engineers; and (v) access other informational resources to resolve issues with the Service.

3.3. Cloudflare will make available a dedicated team of telephone support engineers, to whom Customer may report and resolve potential Issues.

3.4. Additional information regarding support options may be found at http://www.cloudflare.com/help.

4. SCOPE OF CUSTOMER SUPPORT

4.1. Cloudflare will provide to Customer the onboarding and technical support services that are associated with Customer's success package as set forth on Cloudflare's website located at https://www.cloudflare.com/success-offerings/.

4.2. Customer support does not include code development or the debugging of Customer's websites or software.

4.3. For security reasons, only Customer's Authorized Users may submit Claims to Cloudflare.

5. CUSTOMER SUPPORT RESPONSE TIMES AND AVAILABILITY

5.1. Cloudflare's initial response times (listed below) vary based on the customer success offering purchased by Customer and the severity of the Claim. Cloudflare is committed to providing a response within the timeframes described below, as measured from Customer initiation of a Claim.

	STANDARD PLAN	PREMIUM PLAN
P1 Issue	< 2 hours	< 1 hour
P2 Issue	< 4 hours	< 2 hours
P3 Issue	< 48 hours	< 24 hours

	STANDARD PLAN	PREMIUM PLAN
P4 Issue	< 48 hours	< 24 hours

If Customer is unsure of the success offering associated with Customer's Cloudflare account, Customer may contact the customer success manager assigned to its account or email success@cloudflare.com for details.

5.2. Emergency Telephone Support is available all day, every day, for P1 Issues only. Online support is available all day, every day, for all other Issues regardless of severity.

5.3. For Customers who have purchased Cloudflare's Security Operations Center Service ("SOC Service") the following notification response times will apply to all security incidents for Services monitored by the SOC Service:

PRIORITY	RESPONSE TIME
P1 Issue	< 30 mins
P2 Issue	< 2 hours
P3 Issue	< 24 hours
P4 Issue	< 24 hours

For purposes of this section only:

- A "**P1 Issue**" means an ongoing attack where Customer's Service is significantly impaired or unavailable.
- A "**P2 Issue**" means a past true-positive attack with a quantifiable impact on Customer's Cloudflare-protected Internet Properties and/or networks.
- A "**P3 Issue**" means a suspected attack on Customer's Cloudflare-protected Internet Properties and or networks (which has been blocked by Cloudflare or has no discernable impact on Customer's Internet Properties and/or networks).
- A "**P4 Issue**" means all security escalations that are not P1, P2, or P3 Issues as defined in this Section 5.3.
- "**Response Time**" is the time it takes for Cloudflare to notify Customer of an attack as measured by Cloudflare from Cloudflare's initial detection of an attack on Customer's Internet Properties and or networks.

Cloudflare will respond to Issues arising from all other Services besides the SOC Service in accordance with the timelines set forth in Section 5.1.

6. RESOLVED QUERIES

6.1. Following Cloudflare's initial response to a Claim, Cloudflare will work with Customer to identify and resolve any and all Issues. Cloudflare will consider a Claim to be resolved if: (a) Customer agrees that the Issue is resolved; (b) The source of the Issue lies with a third party, in which case, Cloudflare will continue to assist Customer and act as a resource to Customer while

Customer works with the third party to resolve such Issue; or (c) Customer does not respond to a query or request from Cloudflare regarding an Issue after seven (7) consecutive calendar days. Notwithstanding the foregoing, with respect to Section 6.1(c) above, Cloudflare will re-open the Issue if Customer contacts Cloudflare any time after the Issue was considered closed by Cloudflare to report that the Issue has not yet been resolved.

7. SERVICE CREDIT CLAIMS

7.1. To be eligible to submit a Claim, Customer must first have notified Cloudflare of the specific Incident and provided notice of its intention to submit a Claim, using one of the methods set forth in Section 3, within five (5) business days following such Incident.

7.2. To submit a Claim, Customer must contact Cloudflare as detailed above in Section 7.1. Customer must provide to Cloudflare, reasonable details and sufficient evidence to support any Claim, including but not limited to, detailed descriptions of an Incident, the duration of such Incident, network traceroutes, the URL(s) affected, and any steps taken, or attempts made, by Customer to resolve the Incident. Customer must submit a Claim before the end of the billing month immediately following the billing month in which the Incident which is the subject of such Claim occurred.

7.3. Cloudflare will use all information reasonably available to it to validate a Claim and make a good faith judgment on whether a Service Credit applies to such Claim.

8. SLA EXCLUSIONS

8.1. This SLA does not apply to any performance or availability issues: (a) Due to events outside of Cloudflare's control, including but not limited to, Issues caused solely by:

- (i) Customer's or its End Users' hardware, software or connectivity issues;
- (ii) corrupted Customer Content;
- (iii) acts or omissions of Customer, its employees, agents, contractors, or vendors; or
- (iv) a third party gaining access to the Service by means of Customer's Authorized Users' accounts or equipment; (b) Caused by Customer's continued use of the Service after Cloudflare has advised Customer to modify such use, if Customer did not modify its use as advised; or (c) Occurring during beta and trial services, unless otherwise agreed to in writing by Cloudflare.

9. SERVICE CREDITS

9.1. The amount and method of calculation of Service Credits is described below in **Section 10**.

9.2. Service Credits are Customer's sole and exclusive remedy for any violation of the Service Levels.

9.3. The total amount of Service Credits awarded in any annual billing period shall not, under any circumstance, exceed six (6) months of the Customer's cumulative total Monthly Fees actually paid to Cloudflare in such annual billing period. If such Service Credits exceed the maximum, Customer shall also have a right to terminate the Services for cause (chronic SLA breach) and receive any such applicable pro-rata refund of pre-paid amounts for the remaining subscription term of the Services.

9.4. Service Credits for this SLA will only be calculated against Customer's fixed Monthly Fees.

10. SERVICE CREDIT CALCULATION

10.1. For any and each Outage Period experienced by Customer during a monthly billing period, Cloudflare will provide a Service Credit calculated in accordance with the formula below that is applicable to the Customer's success package:

$$\text{Premium Plan Service Credit} = \frac{\mathbf{25} \times \text{Outage Period in Minutes} \times \text{Affected Customer Ratio} \times \text{Monthly Fee}}{\text{Scheduled Availability in Minutes}}$$

$$\text{Standard Plan Service Credit} = \frac{\mathbf{10} \times \text{Outage Period in Minutes} \times \text{Affected Customer Ratio} \times \text{Monthly Fee}}{\text{Scheduled Availability in Minutes}}$$

10.2. RESERVED.

11. METHODOLOGY

11.1. Cloudflare is not responsible for the comprehensive monitoring of Customer Content, and such responsibility lies with Customer. Cloudflare will review and consider all supporting data on a reported Unscheduled Service Outage, provided to it by Customer provided that such data was obtained using a commercially reasonable independent measurement system used by Customer.

11.2. Cloudflare will use all information reasonably available to it in order to calculate the Affected Customer Ratio during an Outage Period. This includes, but is not limited to, Cloudflare's analysis of service data immediately prior to the Outage Period, in order to estimate the ratio of Customer's visitors who were affected during an Outage Period, at one or more of Cloudflare's global data centers.

11.3. If Customer reports verified Unscheduled Service Outages (as defined in the SLA) that result in the Affected Customer Ratio (as defined in the SLA) exceeding 50% three (3) times in four (4) consecutive months, Customer may terminate this Agreement by providing written notice to Supplier within five (5) business days of such third (3rd) (or any subsequent) exceedance within such four (4) month period.

Questions?

If you have questions about these terms or anything else about Cloudflare, please don't hesitate to contact us:

+1 (650) 319-8930

Cloudflare, Inc.
101 Townsend St,
San Francisco, CA 94107
USA

Attachment D

CLOUDFLARE DATA PROCESSING ADDENDUM

Cloudflare, Inc. ("**Cloudflare**") and the North Carolina Department of Information Technology ("**Customer**") have entered into an Addendum, which includes Cloudflare's Agreement, as modified, for the Services provided by Cloudflare (the **"Agreement"**). This Data Processing Addendum**,** including the appendices (the "**DPA**"**)**, forms part of the Agreement.

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

DATA PROCESSING TERMS

This DPA applies where Cloudflare processes Personal Data as a Processor (or sub-Processor as applicable) on behalf of Customer to provide the Services and such Personal Data is subject to Applicable Data Protection Laws (as defined below).

The parties have agreed to enter into this DPA in order to ensure that appropriate safeguards are in place to protect such Personal Data in accordance with Applicable Data Protection Laws. Accordingly, Cloudflare agrees to comply with the following provisions with respect to any Personal Data that it processes as a Processor (or sub-Processor as applicable) on behalf of Customer.

1. Definitions

1.1 The following definitions are used in this DPA:

a) "**Adequate Country**" RESERVED.

b) "**Affiliate**" means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists).

c) "**Applicable Data Protection Laws**" means all laws and regulations that are applicable to the processing of Personal Data under the Agreement, including United States Data Protection Laws.

d) "**Cloudflare Group**" means Cloudflare and any of its Affiliates.

e) "**Controller**" means an entity that determines the purposes and means of the processing of Personal Data, and includes "controller," "business," or analogous term as defined under the Applicable Data Protection Laws.

f) "**Customer Group**" means Customer and any of its Affiliates.

g) "**EU SCCs**" RESERVED.

h) "**Data Privacy Framework**" RESERVED.

i) "**European Data Protection Laws** RESERVED.

j) "**Personal Data**" means all data which is defined as '*personal data*', '*personal information*', or '*personally identifiable information*' (or analogous term) under Applicable Data Protection Laws.

k) "**processing**", "**data subject**", and "**supervisory authority**" shall have the meanings ascribed to them by Law.

l) "**Processor**" means an entity which processes Personal Data on behalf of the Controller, including an entity to which another entity discloses a natural individual's personal information for a business purpose pursuant to a written contract that requires the entity receiving the information to only retain, use, or disclose Personal Data information for the purpose of providing the Services, and includes "processor," "service provider," or analogous term defined under the Applicable Data Protection Laws.

m) "**Services**" shall refer to all of the cloud-based solutions offered, marketed or sold by Cloudflare or its authorized partners that are designed to increase the performance, security and availability of Internet properties, applications and networks, along with any software, software development kits and application programming interfaces ("**APIs**") made available in connection with the foregoing.

n) "**Restricted Transfer**" means: (i) where the EU GDPR or Swiss FADP applies, a transfer of Personal Data from the European Economic Area or Switzerland (as applicable) to a country outside of the European Economic Area or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and Information Commissioner (as applicable); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018. For the avoidance of doubt, a transfer of Personal Data to the United States pursuant to the Data Privacy Framework shall not be a Restricted Transfer.

o) "**UK Addendum**" RESERVED.

p) "**United States Data Protection Laws**" means the United States laws and regulations and the laws and regulations of the State of North Carolina applicable to the processing of Personal Data under the Agreement.

1.2 An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

1.3 For the purposes of this DPA, "to provide" or "providing" the Services means delivering the Services as defined in the Agreement;

2. Status of the parties

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1.

2.2 Each party warrants in relation to Personal Data that it will comply with and provide the same level of privacy protection as required by the Applicable Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties acknowledge and agree that the Customer is the Controller (or a Processor processing Personal Data on behalf of a third-party Controller), and Cloudflare is a Processor (or sub-Processor, as applicable).

2.4 If Customer is a Processor, Customer warrants to Cloudflare that Customer's instructions and actions with respect to the Personal Data, including its appointment of Cloudflare as another Processor and, where applicable have been (and will, for the duration of this DPA, continue to be) authorized by the relevant third-party Controller.

3. Cloudflare obligations

3.1 With respect to all Personal Data it processes in its role as a Processor or sub-Processor, Cloudflare warrants that it shall:

a) only process Personal Data for the limited and specified business purpose of providing the Services and in accordance with: (i) the Customer's written instructions as set out in the Agreement and this DPA, and (ii) the requirements of Applicable Data Protection Laws. In the event Cloudflare is required to process Personal Data under Applicable Data Protection Laws, Cloudflare shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b) not use the Personal Data for the purposes of marketing or advertising;

c) implement appropriate technical and organizational measures as required by the terms of the Agreement between the parties to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex 2 ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Cloudflare may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Service. NOTE that for all purposes the security requirements set forth in Attachment A supersede this subsection.

d) ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under contractual or statutory obligations of confidentiality;

e) as required by the terms of the Agreement, notify the Customer upon becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed for the purpose of providing the Services to Customer by Cloudflare, its sub-Processors, or any other identified or unidentified third party (a "**Personal Data Breach**") and provide the Customer with reasonable cooperation and assistance in respect of that Personal Data Breach, including all reasonable

information in Cloudflare's possession concerning such Personal Data Breach insofar as it affects the Personal Data;

f) not make any public announcement about a Personal Data Breach (a "**Breach Notice**") without the prior written consent of the Customer, unless required by applicable law;

g) to the extent Cloudflare is able to verify that a data subject is associated with the Customer, promptly notify the Customer if it receives a request from a data subject to exercise any data protection rights (including rights of access, rectification or erasure) in respect of that data subject's Personal Data (a "**Data Subject Request**"). Cloudflare shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees;

h) to the extent Cloudflare is able, and in line with applicable law, provide reasonable assistance to Customer in responding to a data subject request to exercise any data protection rights under Applicable Data Protection Laws (including rights of access, rectification or erasure) in respect of that data subject's Personal Data if the Customer does not have the ability to address a Data Subject Request without Cloudflare's assistance. The Customer is responsible for verifying that the requestor is the data subject in respect of whose Personal Data the request is made. Cloudflare bears no responsibility for information provided in good faith to Customer in reliance on this subsection. Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance; ;

i) other than to the extent required to comply with applicable law, following termination or expiry of the Agreement or completion of the Service, at the choice of Customer, delete or return all Personal Data (including copies thereof) processed pursuant to this DPA;

j) taking into account the nature of processing and the information available to Cloudflare, provide such assistance to the Customer as the Customer reasonably requests in relation to Cloudflare's obligations under Applicable Data Protection Laws with respect to:

   (i) data protection impact assessments and prior consultations (as such terms are defined in Applicable Data Protection Laws);

   (ii) notifications to the supervisory authority under Applicable Data Protection Laws and/or communications to data subjects by the Customer in response to any Personal Data Breach; and

   (iii) the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to the security of processing;

   provided that the Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance unless otherwise required by Law; and

k) notify Customer if, in Cloudflare's opinion, any instructions provided by the Customer under clause 3.1(a) infringe Applicable Data Protection Laws, or if Cloudflare otherwise makes a determination that it can no longer meet its obligations under Applicable Data Protection Laws

3.2 RESERVED.

3.3 Cloudflare certifies that it understands and will comply with the obligations and restrictions in clauses 2 (Status of the Parties) and 3 (Cloudflare Obligations), and the Applicable Data Protection Laws.

4. Sub-processing

4.1 Cloudflare will disclose Personal Data to sub-Processors only for the specific purpose of providing the Services.

4.2 Cloudflare will ensure that any sub-Processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-Processor terms (i.e., data protection obligations) that are no less protective of Personal Data than those imposed on Cloudflare in this Agreement (the "**Relevant Terms**"). Cloudflare shall procure the performance by such sub-Processor of the Relevant Terms and shall be liable to the Customer for any breach by such sub-Processor of any of the Relevant Terms.

4.3 The Customer grants a general written authorization: (a) to Cloudflare to appoint other members of the Cloudflare Group as sub-Processors, and (b) after prior notice in accordance with the sub-Processor notification protocol below, to Cloudflare and other members of the Cloudflare Group to appoint third party data center operators, and business, engineering and customer support providers as sub-Processors to support the performance of the Service.

4.4 Cloudflare will maintain a list of sub-Processors at https://www.cloudflare.com/gdpr/subprocessors/ and will add the names of new and replacement sub-Processors to the list at least thirty (30) days prior to the date on which those sub-Processors commence processing of Personal Data. If Customer objects to any new or replacement sub-Processor on reasonable grounds related to data protection, it shall notify Cloudflare of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If Cloudflare is reasonably able to provide the Service to the Customer in accordance with the Agreement without using the sub-Processor and decides in its discretion to do so, then Customer will have no further rights under this clause 4.4 in respect of the proposed use of the sub-Processor. If Cloudflare, in its discretion, requires use of the sub-Processor and is unable to satisfy Customer's objection regarding the proposed use of the new or replacement sub-Processor, then Customer may terminate the applicable Order Form effective upon the date Cloudflare begins use of such new or replacement sub-Processor solely with respect to the Service(s) that will use the proposed new sub-Processor for the processing of Personal Data. If Customer does not provide a timely objection to any new or replacement sub-Processor in accordance with this clause 4.4, Customer will be considered to have consented to the sub-Processor and waived its right to object.

5. Audit and records

5.1 Cloudflare shall, in accordance with the terms of the Agreement and Applicable Data Protection Laws, make available to Customer such information in Cloudflare's possession or control as Customer may reasonably request with a view to demonstrating Cloudflare's compliance with the obligations of Processors under Applicable Data Protection Laws in relation to its processing of Personal Data.

5.2 Cloudflare may fulfill Customer's right of audit under Applicable Protection Laws in relation to Personal Data, by providing:

a) an audit report not older than twelve (12) months, prepared by an independent external auditor demonstrating that Cloudflare's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard;

b) additional information in Cloudflare's possession or control to a data protection supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by Cloudflare under this DPA; and

c) To the extent that Customer's Personal Data is subject to the EU SCCs and the information made available pursuant to this clause 5.2 is insufficient, in Customer's reasonable judgment, to confirm Cloudflare's compliance with its obligations under this DPA or Applicable Data Protection Laws, then Cloudflare shall enable Customer to request one onsite audit per annual period during the Term (as defined in the Main Agreement) to verify Cloudflare's compliance with its obligations under this DPA in accordance with clause 5.3.

5.3 The following additional terms shall apply to audits the Customer requests:

(a) Customer must send any requests for reviews of Cloudflare's audit reports to customer-compliance@cloudflare.com.

(b) Following receipt by Cloudflare of a request for audit under clause 5.2(c), Cloudflare and Customer will discuss and agree in advance on the reasonable start date, scope, duration of, and security and confidentiality controls applicable to any audit under clause 5.2(c). Whenever possible, evidence for such an audit will be limited to the evidence collected for Cloudflare's most recent third-party audit. RESERVED.

(c) Unless otherwise required by Law, Cloudflare may charge a fee (based on Cloudflare's reasonable costs) for any audit under clause 5.2(c). Cloudflare will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(d) Cloudflare may object in writing to an auditor appointed by Customer to conduct any audit under clause 5.2(c) if the auditor is, in Cloudflare's reasonable opinion, not suitably qualified or independent, or a competitor of Cloudflare. Any such objection by Cloudflare will require Customer to appoint another auditor. If the EU SCCs (including as they may be amended in clause 6.2 below) applies, nothing in this clause 5.3 varies or modifies the EU SCCs nor affects any supervisory authority's or data subject's rights under the EU SCCs.

6. Data transfers from the EEA, Switzerland, and the UK – RESERVED.

7. Third Party Data Access Requests

7.1 If Cloudflare becomes aware of any third party legal process requesting Personal Data that Cloudflare processes on behalf of Customer in its role as Processor or sub-Processor (as applicable) then Cloudflare will:

a) immediately notify Customer of the request unless such notification is legally prohibited;

b) inform the third party that it is a Processor or sub-Processor (as applicable) of the Personal Data and is not authorized to disclose the Personal Data without Customer's consent;

c) disclose to the third party the minimum necessary Customer contact details to allow the third party to contact the Customer and instruct the third party to direct its data request to Customer; and

d) to the extent Cloudflare provides access to or discloses Personal Data in response to third party legal process either with Customer authorization or due to a mandatory legal compulsion, then Cloudflare will disclose the minimum amount of Personal Data to the extent it is legally required to do so and in accordance with the applicable legal process.

7.2 In Cloudflare's role as a Processor or sub-Processor, as applicable, it may be subject to third party legal process issued by a government authority (including a judicial authority) requesting access to or disclosure of Personal Data. If Cloudflare becomes aware of any third party legal process issued by a government authority (including a judicial authority) requesting Personal Data that Cloudflare processes on behalf of Customer in its role as Processor or sub-Processor (as applicable) then, to the extent that Cloudflare reviews the request with reasonable efforts and as a result is able to identify that such third party legal process requesting Personal Data raises a conflict of law, Cloudflare will:

a) take all actions identified in clause 7.1 above;

b) pursue legal remedies prior to producing Personal Data up to an appellate court level; and

c) not disclose Personal Data until (and then only to the extent) required to do so under applicable procedural rules.

7.3 Clauses 7.1 and 7.2 shall not apply in the event that Cloudflare has a good-faith belief the government request is necessary due to an emergency involving the danger of death or serious physical injury to an individual. In such event, Cloudflare shall notify Customer of the data disclosure as soon as possible following the disclosure and provide Customer with full details of the same, unless such disclosure is legally prohibited.

7.4 Cloudflare will provide Customer with regular updates about third party legal process requesting Personal Data in the form of Cloudflare's semiannual Transparency Report, which is available at https://www.cloudflare.com/transparency/.

7.5 As of the date Customer entered into this DPA with Cloudflare, Cloudflare makes the commitments listed below. Cloudflare will update these commitments as may be required at https://www.cloudflare.com/transparency/:

a) Cloudflare has never turned over our encryption or authentication keys or our customers' encryption or authentication keys to anyone.

b) Cloudflare has never installed any law enforcement software or equipment anywhere on our network.

c) Cloudflare has never provided any law enforcement organization a feed of our customers' content transiting our network.

d) Cloudflare has never weakened, compromised, or subverted any of its encryption at the request of law enforcement or another third party.

8. General

8.1 This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict

between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

8.2 Cloudflare's liability under or in connection with this DPA, including under the EU SCCs, is subject to the exclusions and limitations on liability contained in the Agreement. In no event does Cloudflare limit or exclude its liability towards data subjects or competent data protection authorities.

8.3 Except where and to the extent expressly provided in the Applicable Data Protection Laws, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

8.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws as specified in the Agreement, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts specified in the Agreement.

8.5 If any provision of this DPA is, for any reason, held to be invalid or unenforceable, the other provisions of the DPA will remain enforceable. Without limiting the generality of the foregoing, Customer agrees that clause 8.2 (Limitation of Liability) will remain in effect notwithstanding the unenforceability of any provision of this DPA.

8.6 RESERVED.

8.7 The Parties have agreed to remove references to foreign data privacy law in the Agreement as they are not applicable to Customer's Internet Properties and operations conducted thereon. If any foreign data privacy laws become implicated per Customer's operations and its use of the Services (including, but not limited to, GDPR and Swiss data privacy laws), Customer agrees, in good faith, to execute a reasonably revised DPA with Cloudflare premised upon the standard Cloudflare DPA found on its website.

Annex 1

Data Processing Description

This Annex 1 forms part of the DPA and describes the processing that Cloudflare will perform on behalf of Customer.

A. LIST OF PARTIES

Data exporter(s): *Customer to complete the right-hand column.*

1.	Name: *Customer and any Customer Affiliates described in the Agreement.*	As stated in the Agreement
	Address: *Addresses of Customer and any Customer Affiliates described in the Agreement (or otherwise notified by Customer to Cloudflare)*	As stated in the Agreement
	Contact person's name, position and contact details:	As stated in the Agreement
	Activities relevant to the data transferred under this DPA and the EU SCCs:	Use of the Service pursuant to the Agreement.
	Signature and date:	This Annex 1 shall be considered executed upon execution of the Addendum.
	Role (controller/processor):	Controller (or Processor on behalf of a third-party Controller).

Data importer(s):

1.	Name:	Cloudflare, Inc.
	Address:	101 Townsend Street San Francisco, CA 94107 USA
	Contact person's name, position and contact details:	Emily Hancock Data Protection Officer legal@cloudflare.com

	Activities relevant to the data transferred under this DPA and the EU SCCs:	Processing necessary to provide the Service to Customer, pursuant to the Main Agreement.
	Signature and date:	This Annex 1 shall be considered executed upon execution of the Addendum.
	Role (controller/processor):	Processor (or sub-Processor)

B. DESCRIPTION OF DATA PROCESSING AND TRANSFER

Categories of data subjects whose Personal Data is transferred:	Natural persons that (i) access or use Customer's domains, networks, websites, application programming interfaces ("APIs"), and applications, or (ii) Customers' employees, agents, or contractors who access or use the Services, such as Cloudflare Zero Trust end users, (together, "End Users"). Natural persons with login credentials for a Cloudflare account and/or those who administer any of the Services for a Customer ("Administrators").
Categories of Personal Data transferred:	In relation to End Users: ● Any Personal Data processed in Customer Logs, such as IP addresses, and in the case of Cloudflare Zero Trust, Cloudflare Zero Trust end user names and email addresses. "Customer Logs" means any logs of End Users' interactions with Customer's Internet Properties and the Service that are made available to Customer via the Service dashboard or other online interfaces during the Term by Cloudflare. ● Any Personal Data processed in Customer Content, the extent of which is determined and controlled by the Customer in its sole discretion. "Customer Content" means any files, software, scripts, multimedia images, graphics, audio, video, text, data, or

	other objects originating or transmitted from or processed by any Internet Properties owned, controlled or operated by Customer or uploaded by Customer through the Service, and routed to, passed through, processed and/or cached on or within, Cloudflare's network or otherwise transmitted or routed using the Service by Customer. In relation to Administrative Users: ● Any Personal Data processed in Administrative User audit logs, such as IP addresses and email addresses.
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, for instance, strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Customer, its End Users, Administrators, and/or other partners may upload content to Customer's online properties which may include special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life. Any such special categories of data shall be protected by applying the security measures described in Annex 2.
The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):	Continuous for the duration of the Main Agreement.
Nature of the processing:	Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Agreement and this DPA.
Purpose(s) of the data transfer and further processing:	Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Agreement and this DPA.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Agreement (to the extent applicable).
For transfers to (sub-) Processors, also specify subject matter, nature and duration of the processing:	The subject matter, nature and duration of the processing shall be as specified in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY (Reserved).

Annex 2

Technical and Organizational Security Measures

Cloudflare has implemented and shall maintain an information security program in accordance with ISO/IEC 27000 standards. Cloudflare's security program shall include:

Measures of encryption of Personal Data

Cloudflare implements encryption to adequately protect Personal Data using:

- state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- trustworthy public-key certification authorities and infrastructure;
- effective encryption algorithms and parameterization, such as a minimum of 128-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Cloudflare enhances the security of processing systems and services in production environments by:

- employing a code review process to increase the security of the code used to provide the Services; and testing code and systems for vulnerabilities before and during use;
- maintaining an external bug bounty program;
- using checks to validate the integrity of encrypted data, and
- employing preventative and reactive intrusion detection.

Cloudflare deploys high-availability systems across geographically-distributed data centers.

Cloudflare implements input control measures to protect and maintain the confidentiality of Personal Data including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authenticating authorized personnel using unique authentication credentials (passwords) and hard tokens;
- automatically signing-out user IDs after a period of inactivity;
- protecting the input of data, as well as the reading, alteration and deletion of stored data; and
- requiring that data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked and secure.

Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

Cloudflare implements measures to ensure that Personal Data is protected from accidental destruction or loss, including by maintaining:

- disaster-recovery and business continuity plans and procedures;
- geographically-distributed data centers;
- redundant infrastructure, including power supplies and internet connectivity;
- backups stored at alternative sites and available for restore in case of failure of primary systems; and

- incident management procedures that are regularly tested.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Cloudflare's technical and organizational measures are regularly tested and evaluated by external third-party auditors as part of Cloudflare's Security & Privacy Compliance Program. These may include annual ISO/IEC 27001 audits; AICPA SOC 2 Type II; PCI DSS Level 1; and other external audits. Measures are also regularly tested by internal audits, as well as annual and targeted risk assessments.

Measures for user identification and authorization

Cloudflare implements effective measures for user authentication and privilege management by:

- applying a mandatory access control and authentication policy;
- applying a zero-trust model of identification and authorization;
- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- allocating and managing appropriate privileges according to role, approvals, and exception management; and
- applying the principle of least privilege access.

Measures for the protection of data during transmission

Cloudflare implements effective measures to protect Personal Data from being read, copied, altered or deleted by unauthorized parties during transmission, including by:

- using state-of-the-art transport encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- using trustworthy public-key certification authorities and infrastructure;
- implementing protective measures against active and passive attacks on the sending and receiving systems providing transport encryption, such as adequate firewalls, mutual TLS encryption, API authentication, and encryption to protect the gateways and pipelines through which data travels, as well as testing for software vulnerabilities and possible backdoors;
- employing effective encryption algorithms and parameterization, such as a minimum of 128-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms;
- using correctly implemented and properly maintained software, covered under a vulnerability management program, and tested for conformity by auditing;
- enforcing secure measures to reliably generate, manage, store and protect encryption keys; and
- audit logging, monitoring, and tracking data transmissions.

Measures for the protection of data during storage

Cloudflare implements effective measures to protect Personal Data during storage, controlling and limiting access to data processing systems, and by:

- using state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- using trustworthy public-key certification authorities and infrastructure;
- testing systems storing data for software vulnerabilities and possible backdoors;
- employing effective encryption algorithms and parameterization, such as requiring all disks storing Personal Data to be encrypted with AES-XTS using a key length of 128-bits or longer.
- using correctly implemented and properly maintained software, covered under a vulnerability management program, and tested for conformity by auditing;
- enforcing secure measures to reliably generate, manage, store and protect encryption keys;
- identifying and authorizing systems and users with access to data processing systems;
- automatically signing-out users after a period of inactivity; and
- audit logging, monitoring, and tracking access to data processing and storage systems.

Cloudflare implements access controls to specific areas of data processing systems to ensure only authorized users are able to access the Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- applying a zero-trust model of user identification and authorization;
- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- monitoring actions of those authorized to delete, add or modify Personal Data;
- release data only to authorized persons, including the allocation of differentiated access rights and roles; and
- controlling access to data, with controlled and documented destruction of data.

Measures for ensuring physical security of locations at which Personal Data are processed

Cloudflare maintains and implements effective physical access control policies and measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers, and related hardware) where the Personal Data are processed or used, including by:

- establishing secure areas;
- protecting and restricting access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to data centers where Personal Data are hosted are logged, monitored, and tracked; and
- data centers where Personal Data are hosted are secured by security alarm systems, and other appropriate security measures.

Measures for ensuring events logging

Cloudflare has implemented a logging and monitoring program to log, monitor and track access to personal data, including by system administrators and to ensure data is processed in accordance with instructions received. This is accomplished by various measures, including:

- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- applying a zero-trust model of user identification and authorization;
- maintaining updated lists of system administrators' identification details;
- adopting measures to detect, assess, and respond to high-risk anomalies;
- keeping secure, accurate, and unmodified access logs to the processing infrastructure for twelve months; and
- testing the logging configuration, monitoring system, alerting and incident response process at least once annually.

Measures for ensuring system configuration, including default configuration

Cloudflare maintains configuration baselines for all systems supporting the production data processing environment, including third-party systems. Configuration baselines should align with industry best practices such as the Center for Internet Security (CIS) Level 1 benchmarks. Automated mechanisms must be used to enforce baseline configurations on production systems, and to prevent unauthorized changes. Changes to baselines are limited to a small number of authorized Cloudflare personnel and must follow change control processes. Changes must be auditable and checked regularly to detect deviations from baseline configurations.

Cloudflare configures baselines for the information system using the principle of least privilege. By default, access configurations are set to "deny-all," and default passwords must be changed to meet Cloudflare's policies prior to device installation on the Cloudflare network, or immediately after software or operating system installation. Systems are configured to synchronize system time clocks based on International Atomic Time or Coordinated Universal Time (UTC), and access to modify time data is restricted to authorized personnel.

Measures for internal IT and IT security governance and management

Cloudflare maintains internal policies on the acceptable use of IT systems and general information security. Cloudflare requires all employees to undertake general security and privacy awareness training at least every year. Cloudflare restricts and protects the processing of Personal Data, and has documented and implemented:

- a formal Information Security Management System (ISMS) in order to protect the confidentiality, integrity, authenticity, and availability of Cloudflare's data and information systems, and to ensure the effectiveness of security controls over data and information systems that support operations; and
- a formal Privacy Information Management System (PIMS) in order to protect the confidentiality, integrity, authenticity, and availability of the policies and procedures supporting Cloudflare's global managed network, as both a processor and a controller of customer information.

Cloudflare will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Cloudflare shall take reasonable steps to

ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Annex 2.

Measures for certification/assurance of processes and products

The implementation of Cloudflare's ISMS and related security risk management processes have been externally certified to the industry-standard ISO/IEC 27001. The implementation of Cloudflare's comprehensive PIMS has been externally certified to the industry-standard ISO/IEC 27701, as both a processor and controller of customer information.

Cloudflare maintains PCI DSS Level 1 compliance for which Cloudflare is audited annually by a third-party Qualified Security Assessor. Cloudflare has undertaken other certifications such as the AICPA SOC 2 Type II certification in accordance with the AICPA Trust Service Criteria, and details of these and other certifications that Cloudflare may undertake from time to time will be made available on Cloudflare's website.

For transfers to (sub-) Processors, the table below describes the specific technical and organizational measures to be taken by the (sub-) Processor to be able to provide assistance to the controller (and, for transfers from a Processor to a sub-Processor, to the data exporter).

Measure	Description
Self-service access to meet data subject rights of access, erasure, rectification etc.	Ability to login to review and edit Personal Data via the Cloudflare dashboard.