Appspace End User License Agreement

Last updated on July 10, 2025

This Appspace End User License Agreement (this **"Agreement"**) is entered into by and between the Customer, on behalf of itself and its Affiliates (**"Customer"**) and Appspace, Inc., a corporation formed under the laws of the state of Delaware, with offices located at 400 N Tampa Street, Suite 1725, Tampa, FL 33602, USA, on behalf of itself and its Affiliates (**"Appspace"**). If Customer is agreeing to this Agreement not as an individual, but on behalf of Customer's company, then "Customer" means Customer's company and by entering into this Agreement, Customer is agreeing to bind, and representing that Customer has full authority to bind, Customer's company to this Agreement. Customer and Appspace may be referred to individually as a **"Party"** and collectively as the **"Parties."**

1. General Terms Overview

1.1. Account Terms. This Agreement governs all Customer's purchases of the Products (as defined below) and incorporates the following exhibits:

- Acceptable Use Policy (**"AUP"**)
- Any ordering documentation (**"Order"**)
- Appspace Service Level Agreement
- Appspace Professional Services Agreement
- Data Processing Addendum
- Data Security Exhibit
- AI Terms Exhibit.

All exhibits listed above can be found at www.appspace.com/legal/

"Affiliate" in this Agreement, means, with respect to any entity, any other person or entity, which, directly or indirectly, owns or controls, is owned or is controlled by or is under common ownership or control with the specified entity, where "control", with respect to any specified entity, means the power to direct the management or affairs of that entity, directly or indirectly, whether through the ownership of voting securities or other beneficial interest, by contract or otherwise.

1.2. Types of Appspace Products. This Agreement governs (a) Appspace's commercially available software products that may be downloaded and installed locally, hosted or cloud-based solutions, including any APIs included therein (collectively, **"Subscription Services"**), and (b) any related support or maintenance services provided by Appspace, including Support and Maintenance Services (as defined in Section 5.1 below) or Professional Services (as defined in Section 5.2 below) (collectively, **"Services"**). Subscription Services, together with any related Appspace standard documentation (**"Documentation"**), and any Services are referred to herein as **"Products"**. All Documentation is available at https://docs.appspace.com/ (or any such successor website provided by Appspace to Customer). If applicable, all hardware provided by Appspace in conjunction with an Order for the Products shall be governed by Appspace's Hardware Policy, which is available upon request.

1.3. Account Registration. Customer may need to register for an Appspace account in order to access or receive any Products. Customer can register for an Appspace account through Appspace's web site located at https://www.appspace.com/. Any registration information that Customer provides to Appspace must be accurate, current, and complete. Customer must also update

Customer's information so that Appspace may send notices, statements and other information to Customer by email or through Customer's account.

2. Product Terms

2.1. Subscription Services Usage Rights. Subject to the terms and conditions of this Agreement, Appspace grants Customer a worldwide, non-exclusive, non-sublicensable and non-transferable right to access and use the Subscription Services for its internal business purposes during the Subscription Term (as defined below) specified in the applicable Order and in accordance with this Agreement.

2.2. Use of Products. Customer at its own cost and expense, unless otherwise set forth in an applicable Order, shall at all times be solely responsible for obtaining and maintaining all required operating system software, hardware, equipment, accessories, network connectivity and any other system elements necessary to meet the minimum system requirements for setup, maintenance, and use of the Products, as described in any Documentation, which may be updated by Appspace from time to time in its sole discretion, and as otherwise set forth in this Agreement. Customer acknowledges that Products may not operate in accordance with specifications if such minimum system requirements are not met. Appspace shall not be responsible for any adverse consequence or loss whatsoever due to Customer's failure to adhere to such minimum system requirements.

2.3. New Releases. Customer acknowledges that Appspace may make updates and enhancements to the Products from time to time. Such enhancements may include New Releases that Customer may use when provided by Appspace during a valid Subscription Term in the same way that Customer uses Products. New Releases will be and are included in the definition of Products in that case. **"New Releases"** are bug fixes, patches, major or minor releases, or any other changes, enhancements, or modifications to the Products that Appspace makes generally commercially available to customers at no additional cost. New Releases will not include new products that are developed by Appspace, which may be purchased for additional cost. Customers using Products that are hosted on the Customer's premises should always use and upgrade to the most current version of the Products.

2.4. No-Charge Products. Appspace may offer certain Products to Customer at no charge, including free accounts, trial use, and access to pre-release, beta or limited release products (collectively, **"No-Charge Products"**). Customer's use of No-Charge Products is subject to any additional terms that Appspace specifies and is only permitted for the period designated by Appspace. Customer understands that No-Charge Products are still under development, may be inoperable or incomplete and are likely to contain more errors and bugs than generally available Products. Customer may not use No-Charge Products for competitive analysis. Appspace may terminate Customer's right to use No-Charge Products at any time and for any reason in Appspace's sole discretion, without liability to Customer. TO THE MAXIMUM EXTENT PERMITTED BY LAW, APPSPACE DISCLAIMS ALL REPRESENTATIONS, WARRANTIES, INCLUDING ANY WARRANTY OF NON-INFRINGEMENT, TITLE, FITNESS FOR A PARTICULAR PURPOSE, FUNCTIONALITY, OR MERCHANTABILITY, WHETHER EXPRESS, IMPLIED, OR STATUTORY, OBLIGATIONS OR LIABILITIES WITH RESPECT TO ANY NO-CHARGE PRODUCT, INCLUDING ANY SUPPORT AND MAINTENANCE SERVICES, WARRANTY, AND INDEMNITY OBLIGATIONS, OR, THAT THE NO-CHARGE PRODUCTS WILL BECOME GENERALLY AVAILABLE.

2.5. Removals and Suspensions. Appspace may (a) remove any Harmful Code contained within Customer Data from the Products, or (b) suspend Customer's access to the Products based on (i) Customer's violation of this Agreement, (ii) in response to a valid Digital Millennium Copyright Act takedown request, (iii) Customer's use of the Products represents an imminent threat to Appspace's network, or (iv) the security or proper function of the Products may be compromised due to hacking, denial of service attacks or other activities of a similar nature. To the extent reasonably practicable given the nature of the issue giving rise to the suspension, Appspace will promptly: (1) notify Customer of such suspension in writing, and (2) reinstate the suspended Products after the issue is abated. Customer will continue to be charged for the Products during any suspension period; provided however that if it is determined that Customer did not violate any terms of this Agreement, then Customer's subscription term shall be extended for a period of time equal to the time of the

suspension at no additional charge. Appspace has no liability to Customer for removing or deleting Customer Data from or suspending Customer access to any Products as described in this Section 2.5 (Removals and Suspension).

3. Ownership and Responsibilities

3.1. Appspace Ownership. Except for the limited licenses granted herein, Appspace and its licensors have and retain all right, title and interest including all intellectual property rights, in and to the Products. No rights are granted to Customer other than as expressly set forth in this Agreement.

3.2. Licensed Users and Devices. Only the specific number of licensed Users or Devices (each as defined below) _ for which Customer has paid the required fees and that Customer designates through the applicable Product may access and use the Product. Some Products may allow Customer to assign a different type of license to Users and Devices, in which case pricing and functionality may vary according to the type. Users may be Customer's, or Customer's Affiliates', employees, representatives, consultants, contractors, agents, or other third parties who are acting for Customer's, or Customer's Affiliates', benefit or on Customer's, or Customer's Affiliates', behalf (**"Users"**). Devices are any screens or displays on which Appspace Subscription Services are displayed publicly (but does not include individual User's computers or mobile devices) (**"Devices"**). Customer may increase the number of Users and Devices permitted to access Customer's instance of the Product by placing a new Order or, in some cases, directly through the Product. In all cases, Customer will pay on a pro-rata basis, the same per User or Device fee, as applicable, in the then current Order. Customer shall be responsible for compliance with this Agreement for all Users and Devices.

3.3. Authorized Users. Customer agrees that (a) only Customer and its Users or Devices are permitted to access and use the applicable Products; (b) it is responsible for acts and omissions of its Users or Devices, including without limitation, its Users' compliance with this Agreement; (c) the usernames and passwords for each User's or Device's account used to access the applicable Product must be kept confidential by User or Device and not shared with unauthorized persons; (d) it is responsible for any and all actions taken using Customer's accounts, usernames and passwords; and (e) it shall notify Appspace as soon as reasonably practical upon becoming aware of any unauthorized access or use of any User or Device account.

3.4. Customer Data. "Customer Data" means any data, content, code, video, images or other materials of any type that Customer uploads, submits or otherwise transmits to or through the Products. Customer will retain all right, title and interest in and to Customer Data in the form provided to Appspace. Subject to the terms of this Agreement, Customer grants to Appspace a non-exclusive, worldwide, royalty-free right (a) to collect, use, copy, store, transmit, modify and create derivative works of Customer Data, in each case solely to the extent necessary to provide the applicable Product to Customer, and (b) to share Customer Data or interact with other people, to distribute and publicly perform and display Customer Data as Customer directs or enables through the Products. Appspace may also access Customer's account, Customer Data or Customer's instance in order to respond to Customer support requests.

3.5. Customer Responsibilities. Customer must ensure that Customer's and its Users' and Devices' use of the Products and all Customer Data is at all times compliant with and all applicable local, state, federal and international laws, rules and regulations (**"Law"**), including as described, and where applicable, in Section 4.2 (Data Protection). This includes Customer acknowledging it will not submit to, store within, or transmit through the Products: (a) any personally identifiable information, except for the limited types expressly set forth in the Data Processing Addendum ("DPA"); (b) medical records and other personal health information as defined under the Health Insurance Portability and Accountability Act of 1996 or any similar federal or state Law; (c) bank account and payment card information and other financial account information; (d) national identifiers; or (e) special categories of data under applicable law (such as racial or ethnic origin, or other political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, home life and sexual orientation) (collectively **"Sensitive Data"**). Customer also acknowledges that Appspace is not acting as Customer's Business Associate or subcontractor (as such terms are defined and used in HIPAA) and that the Products are not HIPAA compliant. "HIPAA" means the Health Insurance Portability and

Accountability Act, as amended and supplemented. Appspace shall have no liability under this Agreement for any Sensitive Data.

3.6. Feedback. From time to time, Customer may choose to submit comments, information, questions, data, ideas, description of processes, or other information to Appspace, including sharing Customer's Add-Ons (defined below) or in the course of using the Products or receiving Services (collectively **"Feedback"**). Appspace will have a royalty-free, worldwide, transferable, sublicensable, irrevocable, and perpetual license to freely use any Feedback, in any manner, without any obligation, payment, or restriction.

3.7. Usage Data. Appspace may collect, analyze and compile internal data based on Customer's use of the Products, including, without limitation, the performance thereof, which shall be aggregated and anonymized (**"Usage Data"**). Usage Data is primarily, and without limitation, for purposes of improving and enhancing the Products, security, diagnostic and/or corrective analytics. Appspace owns all Usage Data and may use such data to the extent permitted under Law and provided such Usage Data does not identify Customer or include Customer's Confidential Information.

3.8. Customer Add-Ons. From time to time, Appspace may, upon written request, allow Customer to develop plugins, extensions, add-ons or other software products or services that interoperate or are integrated with the Products (**"Add-Ons"**). Customer may distribute Customer's Add-Ons to third parties, but only as permitted and agreed in writing by Appspace prior to such distribution. Appspace shall retain all right, title, and interest in and to any Add-Ons developed by Appspace under this Agreement.

3.9. Conditions to Development of Add-Ons. Notwithstanding anything in this Agreement to the contrary, Appspace has no support, warranty, indemnification or other obligation or liability to Customer or to any third party with respect to Customer's Add-Ons or their combination, interaction or use with the Products. Customer shall indemnify, defend and hold Appspace harmless from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with any claim brought against Appspace by a third party relating to Customer's Add-Ons (including any representations or warranties Customer makes about Customer's Add-Ons) or Customer's breach of this Section 3.9 (Customer Development of Add-Ons).

4. Appspace Security and Privacy Responsibility

4.1. Security. Appspace will maintain the information security program described in Data Security Exhibit.

4.2. Compliance Review. Customer shall use the Services in accordance with the quantities listed on the Order Form ("**Usage Limitations**"). Appspace may review compliance by Customer with the Usage Limitations and Customer shall provide reasonable cooperation to that purpose where so required. In the event such process shows a non-compliance, Appspace may charge Customer for such noncompliance in accordance with Section 6.1 below.

4.3. Privacy Policy. Please review Appspace's Privacy Policy for more information on our use and collection of data relating the performance and usage of our Products and websites. In the event of a conflict between the terms of this Agreement and the Privacy Policy, the terms of this Agreement will control.

5. Services

5.1. Support and Maintenance Services. Appspace will provide the support and maintenance services (**"Support and Maintenance Services"**) for Products described in the Appspace Support Definitions. Support and Maintenance Services will be provided at the support level and during the support term specified in the Order. The Appspace Support Definitions incorporates Appspace Service Level Agreement (the **"SLA"**). Appspace shall provide Customer with the service level credits set forth in the SLA as Customer's sole and exclusive remedy for Appspace's failure to meet the service availability requirements set forth therein. The Appspace Support Definitions may be modified by Appspace from time to time to reflect process improvements or changing practices for Customer's benefit. Appspace supports and provides fixes, patches or any other modifications to major versions of the Products for one year after the first major iteration of that version was released (as an

example, Appspace supports version 5.2.2 for one year after version 5.2.3 was released). In the event of any conflict of terms between the Appspace Support Definitions and this Agreement, the terms within the Appspace Support Definitions shall control.

5.2. Professional Services. Appspace will provide professional services and training services (**"Professional Services"**) purchased in an Order in accordance with the descriptions and conditions for those services set forth in the Order and any accompanying service descriptions or datasheets, if applicable. All Professional Services are subject to the terms and conditions of the Appspace Professional Services Agreement. In the event of any conflict of terms between the Professional Services Agreement and this Agreement, the terms within the Professional Services Agreement shall control.

6. Orders, Payment and Delivery

6.1. Orders from Appspace. Customer's quantities of Users and Devices, listed in each Order cannot be decreased during the term of the applicable Order. Orders can also include any storage, overage or capacity limits and in the event Customer exceeds the stated limits, Appspace may charge the Customer in the form of excess overage fees.

6.2. Orders through a Reseller. This Agreement applies whether Customer purchases the Products directly from Appspace or through any Appspace authorized reseller or distributor (**"Reseller"**). If Customer purchases through a Reseller, Customer's use of the Products shall be as stated in the Order placed by Reseller for Customer, and Reseller is responsible for the accuracy of any such Order. Resellers are not authorized to make any promises or commitments on Appspace's behalf, and Appspace is not bound by any obligations to Customer other than what Appspace specifies in this Agreement.

6.3. Delivery. Appspace will deliver applicable Products login instructions to the email address(es) specified in an Order when Appspace has received payment of all applicable fees. All deliveries will be electronic, and installation is the responsibility of the Customer. Appspace shall have no further delivery obligations after delivery of the license unless stated otherwise.

6.4. Payment. Customer agrees to pay all fees to Appspace in accordance with the terms of each Order. Other than as expressly set forth in Sections 7.5 (Refund or Payment upon Termination) and 10.2 (IP Indemnification by Appspace), all amounts are non-refundable, non-cancelable and non-creditable. In making payments, Customer acknowledges that Customer is not relying on future availability of any Products beyond the current Subscription Term or any New Releases. Subscription Term. If Customer pays by credit card, Customer agrees that Appspace may bill Customer's credit card or invoice Customer for renewals, additional Users and Devices, and unpaid fees, as applicable. If Customer purchases any Products through an Order with a Reseller, Customer owes payment to the Reseller as agreed between Customer and the Reseller, but Customer acknowledges that Appspace may terminate Customer's rights to use Products if Appspace does not receive Appspace's corresponding payment from the Reseller, with at least five (5) business day's prior notice to Customer. In the event the Reseller fails to pay Appspace, Customer agrees to use best efforts to have Appspace paid either by Reseller or Customer. Upon termination, any unpaid payments for performed Services will be accelerated and become immediately due and payable. In addition to any other remedies that Appspace may have at Law or equity, any late payments will be subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by Law, whichever is less. Customer will reimburse Appspace for all reasonable costs incurred in collecting any late payments or interest, including attorney's fees and collection agency fees. **In addition to any other rights or remedies that Appspace may have at Law or in equity, Customer acknowledges that if payment is not made within thirty (30) days of the date of the Order, whether owed directly to Appspace or directly to a Reseller, then, notwithstanding any language to the contrary in this Agreement (including Section 16.8 (Dispute Resolution), or any other agreement which Customer may have with Appspace, Appspace will have the right to terminate or disable all Products with no liability to Customer.**

6.5. Taxes. This Section 6.5 (Taxes) will not apply if Customer placed Customer's Order through a Reseller. Customer will be responsible for all related bank charges, taxes, withholdings, duties and levies in connection with the Products charges (excluding taxes based on the net income

of Appspace). Customer's payments under this Agreement exclude any taxes or duties payable in respect of the Products in the jurisdiction where the payment is either made or received. To the extent that any such taxes or duties are payable by Appspace, Customer must pay to Appspace the amount of such taxes or duties in addition to any fees owed under this Agreement. Notwithstanding the foregoing, Customer may have obtained an exemption from relevant taxes or duties as of the time such taxes or duties are levied or assessed. In that case, Customer will have the right to provide to Appspace any such exemption information, and Appspace will use reasonable efforts to provide such invoicing documents as may enable Customer to obtain a refund or credit for the amount so paid from any relevant revenue authority if such a refund or credit is available.

7. Term and Termination

7.1. Agreement Term. This Agreement is in effect for as long as Customer has a valid Order (the **"Term"**), unless sooner terminated as permitted in this Agreement.

7.2. Subscription Terms and Renewals. Products are provided for a set term specified in an applicable Order. The term of each Product license (the **"Subscription Term"**) will end upon any termination of this Agreement or the applicable Order, regardless of being identified as "perpetual" or if no expiration date is specified. Except as otherwise specified, Subscription Terms will automatically renew for periods equal to the initial term period stated on such Order, unless either Party provides the other with sixty (60) days' written notice prior to the end of the relevant Subscription Term. Unless expressly provided for, such Product renewals will be at Appspace's then current-list price. If Customer upgrades Products prior to the Subscription Term renewal date, then Customer's payment due for the upgraded Products will be prorated and credited based on Customer's remaining Subscription Term and the date on Customer's upgraded invoice will become Customer's new renewal date.

7.3. Termination for Breach. Either Party may terminate this Agreement by written notice to the other Party if the other Party materially breaches any of the terms of this Agreement and does not cure the breach within thirty (30) days after written notice of the breach.

7.4. Termination for Insolvency. Either Party may terminate this Agreement if the other Party ceases to operate, declares bankruptcy, or becomes insolvent or otherwise unable to meet its financial obligations.

7.5. Refund or Payment upon Termination. If this Agreement is terminated by Appspace in accordance with Section 7.3 (Termination for Breach) above, Customer will pay any unpaid fees covering the remainder of the term of all Orders to the extent permitted by Law. If this Agreement is terminated by Customer in accordance with Section 7.3 (Termination for Breach) above, Appspace will refund to Customer any pre-paid but unused fees on a pro-rata basis covering the remainder of the term of all Orders to the extent permitted by Law.

7.6. Effects of Termination. Upon any termination of an applicable Order, Customer will no longer have any right to use or access any Products, or any information or materials that Appspace makes available to Customer under such Order. Upon any termination of an applicable Order, Customer will no longer have any right to use or access any Products, or any information or materials that Appspace makes available to Customer under such Order. Upon any termination of this Agreement, Appspace will delete any Customer Data within ninety (90) days while having no obligation to continue storing such data. The following provisions will survive any termination or expiration of this Agreement: 2.5 (No-Charge Products) (disclaimers and use restrictions only), 3.1 (Appspace Ownership), 3.6 (Customer Restrictions), 3.7 (Feedback), 3.10 (Conditions to Development of Add-Ons), 4.3 (License Certifications and Audits), 6.4 (Payment), 6.5 (Taxes), 7 (Term and Termination), 8.4 (Warranties; Disclaimer), 9 (Confidentiality), 10.1 (Customer Indemnification), 11 (Limitation of Liability), 12.1 (Third Party Materials), 13 (Export Restrictions), 14 (Emergency Alert Systems), and 16 (General).

8. Warranties

8.1. Mutual Warranty. Each Party represents and warrants it has the legal power and authority to enter in this Agreement.

8.2. Appspace Warranty. Appspace warrants that during the valid Subscription Term the Products will function materially in accordance with the related Documentation and, if applicable,

ensure the availability in accordance with the SLA. The warranties provided in this Section 8.2 (Appspace Warranty) will not apply if Customer fails to provide written notice within thirty (30) days after discovery of the breach. If Customer fails to provide such notice, Customer's exclusive remedy of such breach shall be Appspace using diligent efforts to correct the Products so the foregoing warranty is met. This warranty will not apply if the error or non-conformance was caused by (1) the unauthorized use of Products; or (2) if the Product is modified or combined to a non-Appspace product by any party other than Appspace and without Appspace's written approval; or (3) Third-Party Materials.

8.3. Customer Warranty. Customer represents and warrants that: (a) Customer has the necessary and appropriate rights, releases and permissions to provide Customer Data to Appspace, and (b) Customer Data does not and will not infringe or misappropriate any third party right, including any intellectual property rights, privacy rights or violate any Laws.

8.4. Disclaimer. EXCEPT FOR THE LIMITED WARRANTIES IN SECTION 8.2 (APPSPACE WARRANTY), All PRODUCTS ARE PROVIDED "AS-IS," AND "AS AVAILABLE," AND APPSPACE EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES AND REPRESENTATIONS OF ANY KIND, INCLUDING ANY WARRANTY OF NON-INFRINGEMENT, TITLE, FITNESS FOR A PARTICULAR PURPOSE, FUNCTIONALITY, OR MERCHANTABILITY, WHETHER EXPRESS, IMPLIED, OR STATUTORY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, APPSPACE DOES NOT REPRESENT THAT: (A) THE PRODUCTS WILL BE ERROR-FREE; (B) THE PRODUCTS WILL OPERATE IN COMBINATION WITH ANY OTHER HARDWARE, SOFTWARE, SYSTEM, OR DATA; (C) THE PRODUCTS WILL MEET CUSTOMER'S REQUIREMENTS OR EXPECTATIONS; (D) THE PRODUCTS ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS UPON DELIVERY TO CUSTOMER; (E) ANY STORED DATA WILL NOT BE LOST OR CORRUPTED; OR THAT (F) ALL ERRORS IN THE PRODUCTS WILL BE CORRECTED.

9. Confidentiality. Except as otherwise set forth in this Agreement, each Party agrees that all confidential or proprietary business, technical and financial information disclosed to such party (**"Receiving Party"**) by the disclosing Party (**"Disclosing Party"**) constitute the confidential property of the Disclosing Party (**"Confidential Information"**), provided that it is identified as confidential at the time of disclosure, or which should be reasonably understood by Receiving Party as the confidential or proprietary information of Disclosing Party or its Affiliates. Any Products and any performance information relating to the Products shall be deemed Confidential Information of Appspace without any marking or further designation. Except as expressly authorized in this Agreement, the Receiving Party will hold in confidence and not use or disclose any Confidential Information. The Receiving Party's nondisclosure obligation shall not apply to information which the Receiving Party can document: (a) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (b) is or has become public knowledge through no fault of the Receiving Party; (c) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (d) is independently developed by employees of the Receiving Party who had no access to such Confidential Information. The Receiving Party may also disclose Confidential Information if so required pursuant to a Law or court order (but only to the minimum extent required to comply with such regulation or order and with advance notice, if and as permitted by Law, to the Disclosing Party). The Receiving Party acknowledges that disclosure of Confidential Information may cause substantial harm for which damages alone may not be a sufficient remedy; and therefore, that upon any such disclosure or threatened disclosure by the Receiving Party the Disclosing Party shall be entitled to seek appropriate equitable relief (without posting a bond or other security) in addition to whatever other remedies the Disclosing Party might have at Law. For the avoidance of doubt, this Section 9 (Confidentiality) shall not operate as a separate warranty with respect to the operation of any Product. Upon the termination or expiration of this Agreement, each Party shall return or destroy the Confidential Information of the other Party; provided however that (i) any Customer Data within Appspace's system shall not be destroyed for a period of thirty (30) days from the expiration or termination of this Agreement to allow Customer to download or otherwise retrieve such Customer Data; and (ii) either Party may retain backup or archival copies of Confidential Information contained

on electronic drives, provided however that such retained information shall remain subject to the terms of this Agreement. The obligations set forth in this Section 9 (Confidentiality) will terminate three (3) years after the expiration or earlier termination of the Term (as defined below).

10. Indemnification

10.1. Customer Indemnification. Customer will defend, indemnify and hold harmless Appspace from and against any loss, cost, liability or damage, including reasonable attorneys' fees, for which Appspace becomes liable arising from or relating to any claim brought by a third party alleging that Customer Data, or Customer's use of the Subscription Services in violation of this Agreement infringes or misappropriates the intellectual property rights of a third party or violates Law.

10.2. IP Indemnification by Appspace. Appspace will defend Customer against any claim brought against Customer by a third party alleging that a Product, when used as authorized under this Agreement, infringes a valid patent or registered copyright of such third party (a **"Claim"**), and Appspace will indemnify Customer and hold Customer harmless against any damages and costs finally awarded by a court of competent jurisdiction or agreed-to settlement by Appspace (including reasonable attorneys' fees) arising out of a Claim. If Customer's use of a Product is (or in Appspace's opinion is likely to be) enjoined, if required by settlement, or if Appspace determines such actions are reasonably necessary to avoid material liability, Appspace may, at Appspace's option and in Appspace's reasonable discretion: (i) procure a license for Customer's continued use of the Product in accordance with this Agreement; (ii) substitute a substantially functionally similar Product; or (iii) terminate Customer's right to continue using the Product and issue a pro rata refund for any prepaid amounts for the Subscription Services not provided. Appspace's indemnification obligations above under Section 10.2 (IP Indemnification by Appspace) do not apply: (1) if the Product is modified or combined to a non-Appspace product by any party other than Appspace and without Appspace's written approval, but solely to the extent the alleged infringement is caused by such modification; (2) to unauthorized use of Products; (3) to any Claim arising as a result of (y) Customer Data (or circumstances covered by Customer's indemnification obligations in Section 10.1 (Customer Indemnification)) or (z) any Third-Party Materials contained with the Products; (5) to any unsupported release of the Product; or (6) if Customer settles or make any admissions with respect to a Claim without Appspace's prior written consent. THIS SECTION 10.2 (IP INDEMNIFICATION BY APPSPACE) STATES APPSPACE'S SOLE LIABILITY AND CUSTOMER'S EXCLUSIVE REMEDY FOR ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS IN CONNECTION WITH ANY PRODUCT OR OTHER ITEMS PROVIDED BY APPSPACE UNDER THIS AGREEMENT.

10.3. Indemnification Procedures. The indemnification obligations in this Section 10 (Indemnification) are subject to the indemnified Party receiving (a) prompt written notice of such claim (but in any event notice in sufficient time for the indemnifying Party to respond without prejudice); (b) giving the indemnifying Party the exclusive right to control and direct the investigation, defense, or settlement of such claim, provided any such settlement unconditionally releases the indemnified Party of all liability; and (c) all reasonable necessary cooperation by the indemnifying Party, at the indemnifying Party's expense.

11. Limitation of Liability.

11.1. Exclusion of Damages. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY SHALL BE LIABLE FOR ANY LOSS OF USE, LOST DATA, INTERRUPTION OF BUSINESS, COSTS OF DELAY OR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING LOST PROFITS), REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

11.2. Damages Cap. NEITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER SHALL EXCEED THE AMOUNT ACTUALLY PAID BY CUSTOMER UNDER THE APPLICABLE ORDER FOR THE SERVICES IN THE 12 MONTHS IMMEDIATELY PRECEDING THE CLAIM. NOTWITHSTANDING ANYTHING ELSE IN THIS AGREEMENT, APPSPACE'S AGGREGATE LIABILITY TO CUSTOMER IN RESPECT OF NO-CHARGE PRODUCTS SHALL BE TWENTY U.S. DOLLARS ($20 USD).

11.3. Exceptions. THIS SECTION 11 (LIMITATION OF LIABILITY) SHALL NOT APPLY TO (A) AMOUNTS OWED BY CUSTOMER UNDER ANY ORDERS, OR (B) EITHER PARTY'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT; (C) EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; OR (D) EITHER PARTY'S MISAPPROPRIATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY.

11.4 Failure of Essential Purpose. THE PARTIES AGREE THAT THE LIMITATIONS SPECIFIED IN THIS SECTION 11 (LIMITATION OF LIABILITY) WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED ITS ESSENTIAL PURPOSE.

12. Third Party Materials and Code.

12.1. Third Party Materials. Appspace or third parties may from time-to-time display, include, or make available to Customer third-party products or services, including RSS feeds, weather widgets, add-ons and plugins as well as implementation, customization, training, and other consulting services for use with the Products (collectively, **"Third Party Materials"**). If Customer procures any of these Third Party Materials, Customer will do so under a separate agreement (and exchange of data) solely between Customer and the applicable third-party vendor. Representations made regarding Third Party Materials will be governed by the policies and representations made by these third-parties. Appspace does not warrant non-Appspace products or services, whether or not they are designated by Appspace as "verified" or otherwise, and Appspace disclaims all liability for such Third Party Materials. If Customer installs or enables any Third Party Materials or services for use with Products, Customer acknowledges that Appspace may allow the vendors of those products and services to access Customer Data as required for the interoperation and support of such add-ons with the Products. Appspace shall not be responsible for any disclosure, modification or deletion of Customer Data resulting from any such access by third party add-on vendors.

13. Export Restrictions. The Products are subject to export restrictions by the United States government and import restrictions by certain foreign governments, and Customer agrees to comply with all applicable export and import Laws and regulations in Customer's use of the Products. Customer shall not (and shall not allow any third-party to) use, remove or export from the United States or allow the export or re-export of any part of the Products in a U.S.-embargoed country or region or in violation of any U.S. export Laws. Customer represents and warrant that (i) Customer is not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list and (ii) that none of Customer Data is controlled under the US International Traffic in Arms Regulations. The Products are restricted from being used for the design or development of nuclear, chemical, or biological weapons or missile technology without the prior permission of the United States government.

14. Emergency Alert Systems. The Products are not intended to be used in place of an emergency alert system. In the event of an emergency, immediately contact the appropriate emergency services and follow their instructions. Appspace shall not be held responsible and/or liable for any damage, harm, or loss incurred as a result of, the use of, or reliance on the Products during an emergency.

15. Commercial Item Software. The Products are commercial computer software. If Customer is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Products, or any related documentation of any kind, including technical data and manuals, is restricted by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Products were developed fully at private expense. All other use is prohibited

16. General

16.1. Notice. Any notice under this Agreement must be given in writing. Appspace may provide notice to Customer via email or through Customer's account. Notice of updates to terms of use, privacy terms or other terms related to Appspace's website and Products may be delivered by posting such updated on the website. Appspace's notices to Customer will be deemed given upon the first business day after Appspace sends it. Customer may provide notice to Appspace by email at

legal@appspace.com, certified mail, return receipt requested, to Appspace Inc., 382 NW 191st Street, Miami FL 33176, USA, Attn: Legal and Accounting Department. Notice sent to Appspace email will be deemed given upon Appspace sending a reply email acknowledging receipt.

16.2. Force Majeure. Neither Party shall be liable to the other for any delay or failure to perform its obligation under this Agreement (except for a failure to pay fees) if the cause of delay or failure is due to unforeseen events which are beyond the reasonable control of such Party, including, without limitation, a strike, blockade, war, act of terrorism, riot, natural disaster, failure or diminishment of power or telecommunications or data networks or services, or refusal of a license by a government agency. The affected Party shall promptly notify the other Party and make reasonable efforts to mitigate the effects of such event.

16.3. Independent Contractors. The Parties are independent contractors and this Agreement shall not be construed as constituting either Party as a partner of the other or to create any other form of legal association that would give one Party the express or implied right, power or authority to create any duty or obligation of the other Party.

16.4. Assignment. Customer may not assign this Agreement without Appspace's prior written consent. Appspace may assign any of Appspace's rights and obligations under this Agreement (in whole or in part) without Customer's consent.

16.5. Waiver. No failure or delay by the injured Party to this Agreement in exercising any right, power or privilege hereunder shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder at Law or equity.

16.6. Invalidity and Severability. If any provision of this Agreement is held to be void, invalid, unenforceable or illegal, other provisions shall continue in full force and effect.

16.7. Amendment. This Agreement may not be modified or amended by Customer without Appspace's written agreement (which may be withheld in Appspace's complete discretion without any requirement to provide any explanation). Appspace may update or amend this Agreement from time to time. In which case, the new Agreement will supersede any prior versions. Customer's continued use of the Products following the effective date of any such amendment may be relied upon by Appspace as Customer's consent to any such amendment.

16.8. Dispute Resolution. In a claim arising out of, or controversy surrounding this Agreement, the Parties will consult and in good faith negotiate with each other to reach a satisfactory solution to both Parties. Consultations and negotiations will be confidential and treated as a compromise. If the Parties are unable to reach a settlement within ninety (90) days, either Party may pursue relief as available under Section 16.9 (Governing Law; Venue).

16.9. Governing Law; Venue. This Agreement shall be governed by and construed in accordance with the laws of the State of Delaware, USA without regard to the conflict of law provisions thereof. The sole venue for all disputes relating to this Agreement shall be in New Castle County, Delaware, USA.

16.10. Injunctive Relief. Nothing in this Agreement shall prevent either Party from seeking injunctive relief with respect to violation of intellectual property rights, confidentiality obligations or enforcement or recognition of any award or order in any appropriate jurisdiction.

16.11. Exclusion of UN Convention and UCITA. The terms of the United Nations Convention on Contracts for the Sale of Goods do not apply to this Agreement. The Uniform Computer Information Transactions Act (UCITA) shall not apply to this Agreement regardless of when or where adopted.

16.12. Headings. Heading to sections in this Agreement are for the purpose of information and identification only and shall not be construed as forming part of this Agreement.

16.13. Entire Agreement. This Agreement, including any Orders between Appspace and Customer, constitutes the entire agreement between Customer and Appspace relating to the Products and supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the Products or any other subject matter covered by this Agreement. Any inconsistent or conflicting terms and conditions contained in any purchase order or other terms and conditions issued by Customer shall be of no force or effect, even if the terms are accepted by

the Parties. Each party agrees that use of pre-printed forms, including but not limited to email, purchase orders, acknowledgements or invoices, is for convenience only and all pre-printed terms and conditions stated thereon, except as specifically set forth in this Agreement, are void and of no effect.

Acceptable Use Policy

Last updated on July 17, 2024

In order to provide Customer with the best Services and Products, Appspace needs to keep its network and platforms up and running as fast and efficiently as possible. To do this, Appspace needs to make sure that none of its customers abuse or misuse the software or systems. Because Appspace cannot possibly define every situation that can fall under abuse or misuse, Appspace has listed some of the guidelines and do's and don'ts in this Acceptable Use Policy (this **"AUP"**), but this is not intended to be a fully comprehensive list. If something illegal or inconsistent with the Appspace policies occurs on the network or with the Software, Appspace reserves the right to remove the Content and suspend or terminate Customer's account. **"Content"** as used in this AUP means: (1) any information, data, text, software, code, scripts, music, sound, photos, graphics, videos, messages, tags, interactive features, or other materials that Customer posts, uploads, shares, submits, or otherwise provide in any manner to the services and (2) any other materials, content, or data Customer provides to Appspace or use with the Appspace Products or Services.

The AUP is incorporated by reference in the End User License Agreement and/or any related Order Form between Appspace and Customer. Words that are capitalized in this AUP have the meanings given to them in the End User License Agreement and/or any related Order Form.

Most of these guidelines are common sense: do not do anything evil, do not do anything you know you should not do, and do not do anything you would not want someone to do to you.

A. **Account Terms**

1. Customer is responsible for maintaining the security and confidentiality of user IDs and passwords. Customer shall promptly notify Appspace in the event Customer becomes aware of any such breach of the foregoing sentence.

Appspace cannot and will not be liable for any loss or damage from Customer's failure to comply with this security obligation.

2. Customer is responsible for all Content posted on and activity that occurs under Customer's account (even when Customer did not post the Content, but it is posted by others who have access, legal or otherwise, to Customer' account, but not if the Content was posted by Appspace or any Appspace employee, contractor, or agent).
3. Customer understands that the technical processing and transmission of the services, including Customer's Content, may be transferred encrypted and may involve transmissions over public networks; and may also involve changes to conform and adapt to technical requirements of connecting networks or devices.

B. **Prohibited Wrongful Activities; Inappropriate Content and Communications**

1. Customer may not use Appspace Products or Services for any illegal or unauthorized purpose, or to violate any applicable laws (including without limitation data, privacy, and export control laws). By way of further example this includes, but is not limited to, the following:

    - Any activity that violates a person's privacy, including publishing or posting a person's private and confidential information without their express permission, or collecting or gathering a person's personal information (including account names or information) from our services.
    - Any activity that harms, threatens or exploits children or minors (including child pornography, which Appspace will promptly remove and report to law enforcement, including the National Center for Missing and Exploited Children).
    - Any activity that would involve renting, leasing, reproducing, modifying, adapting, creating derivative works of, distributing, selling, sublicensing, transferring, or providing access to the Products to a third party.
    - Using the Products for the benefit of, or on behalf of, any third party.
    - Incorporating any Products into a product or service Customer provides to a third party
    - Any activity intended to reverse engineer, disassemble, decompile, translate, or otherwise seek to obtain or derive the source code, underlying ideas, algorithms, file formats or non-public application programming interfaces to any Products, except as permitted by Law.
    - Any attempt to remove or obscure any proprietary or other notices contained in any Product
    - Any activity that infringes upon the rights of Appspace or others (e.g., unauthorized sharing of music, photographs, logos, or of any other copyrighted or otherwise protected materials (such as those covered by intellectual property rights, trade secrets, or moral, proprietary or contractual rights)).
    - Sending, generating, hosting, posting, or transmitting unsolicited bulk email or instant messages, i.e., spam.

- Publicly displaying inappropriate images, such as nudity, bestiality, pornography/sexually explicit, etc.
- Engaging in activity that is false or misleading, such as attempts to ask for money under false pretenses, impersonating someone else, phishing, spoofing, etc.
- Engaging in activity that is harmful to, or may harm, the Appspace products or others (e.g. interfering with features meant to monitor or limit the number of Users in the Products, viruses, worms, bots, any code of a destructive nature, stalking, hate speech, inciting or advocating violence against others).
- Accessing or searching any part of the services by any means other than our publicly supported interfaces (for example, “scraping”).
- Using meta tags or any other “hidden text” including Appspace’s, or our suppliers’, product names or trademarks.
- Could otherwise cause damage to Appspace or any third party

2. Accounts created or registered by “bots” or any other automated methods are not permitted.
3. Customer may not modify, adapt, or hack the Appspace Products or Services or modify another website so as to falsely imply that such website is associated with Appspace, its website, or any Appspace Products or Services.
4. Customer may not use the Appspace Products or Services if Customer is developing software or services competitive to Appspace, monitoring the Products or Services for performance or functionality, or measuring for any other competitive purposes. Any violation of this clause will be considered a material breach and result in immediate termination of any Appspace Products and Services, and Appspace may pursue any and all remedies available to it in law or equity.
5. Verbal, physical, written, or other abuse (including stalking, harassing, threats of abuse or retribution) against any person or entity, including any Appspace customer, employee, member, or officer is not permitted and may result in immediate account termination.
6. Customer may not engage in activities that could interfere or compromise the integrity or performance of our systems. This could include modifying, disabling, probing, scanning, or testing the vulnerability of any system or network that hosts our Services.
7. Customer may not tamper with, reverse-engineer, or hack our services; and Customer may not circumvent any security or authentication measures, or attempt to gain unauthorized access to the Services, related systems, networks, or data.
8. Deciphering any transmissions to or from the servers running the Services is not permitted.
9. Customer may not overwhelm or attempt to overwhelm the Appspace infrastructure by imposing an unreasonably large load on our systems that consume extraordinary resources (CPUs, memory, disk space, bandwidth, etc.), such as:

- Using “robots,” “spiders,” “offline readers,” or other automated systems to send more request messages to our servers, such as in a DDOS attack, than a human could reasonably send in the same period of time by using a normal browser; or
- Going far beyond the use parameters for any given service as described in its corresponding documentation.

10. Customer may not consume an unreasonable amount of storage for media, such as music, videos, pornography, etc., in a way that is unrelated to the purposes for which the Services were designed. Appspace, in its sole discretion, will determine whether Customer is consuming an unreasonable amount of storage.
11. Customer may not post, upload, store, share, submit, or otherwise provide Content that:
    - Customer does not have the right to submit;
    - Is deceptive, fraudulent, illegal, or may reasonably be perceived as obscene, defamatory, libelous, threatening, harmful to minors, indecent, harassing, or hateful;
    - Encourages illegal or tortious conduct, or that is otherwise inappropriate;
    - Attacks others based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability, medical condition, or other legally protected category;
    - Contains viruses, bots, worms, scripting exploits, Malicious Code, or other similar materials;
    - Is intended to be inflammatory;
    - Contains personally identifiable information, except as necessary for the establishment of Customer’s Appspace account;
    - Contains any patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act of 1996 as amended, or any similar federal or state laws, rules or regulations;
    - Contains information subject to regulation or protection under specific laws such as the Gramm-Leach-Bliley Act or related rules or regulations.
12. Customer also may not solicit our users for commercial purposes, or promote or advertise Products or Services other than Customer’s own, unless expressly permitted by Appspace.

C. API Terms

Customer may access Customer’s Appspace account data via an Application Program Interface (“API”). Any use of the API, including use of the API through a third-party product that accesses Appspace, is bound by the terms of the End User Agreement (www.appspace.com/legal/user-agreement/). Abuse of the API or excessively frequent requests to Appspace via the API may result in the temporary or permanent suspension of Customer’s account access to the API. Appspace, in its sole discretion, will determine abuse or excessive usage of the API.

Without affecting any other remedies available to us, Appspace may permanently or temporarily remove content, or terminate, or suspend a user's account or access to the services without notice or liability if Appspace, in its sole discretion, determines that a user has violated this Acceptable Use Policy. Termination or suspension of a Customer's account will not prevent Customer's obligations to pay fees owed to Appspace.

AI Terms Exhibit

This AI Terms Exhibit ("**AI Terms**") is incorporated into and made a part of the Appspace End User Agreement (or similar document giving the Customer the right to use and access the Subscription Services) entered into by and between Appspace and Customer (the "**Agreement**"). All capitalized terms that are used but not defined in these AI Terms shall have the respective meanings given to them in the Agreement. In the event of a conflict between these AI Terms and the Agreement, these AI Terms will control.

1. AI FEATURES

These AI Terms shall govern Customer's use of certain features within the Subscription Services that are provided using artificial intelligence ("**AI Features**"). The results generated from the AI Features are called the "**Output**" for the purposes of these AI Terms. Customer acknowledges that the AI Features are provided through third-party providers. Appspace's third party providers on the date of these AI Terms are Microsoft, Inc. and Google, LLC, however, Appspace does not commit to the use of any specific third-party providers going forward, and Appspace reserves the right to add or remove third-party providers in its sole discretion. To the extent any third-party provider requires Appspace to pass-through or flow down any terms and conditions to End Users, such additional terms and conditions will be provided to Customer at www.appspace.com/legal.

Customer further acknowledges that Laws around the use of artificial intelligence are rapidly changing. In the event any changes in Law results in Appspace's inability to offer the AI Features, Appspace reserves the right, in its sole discretion, to limit Customer's use of the AI Features in any way Appspace believes will allow it to comply with all Laws, including reduction in features and functionality, or limiting the use of the AI Features in certain geographical locations.

Customer represents and warrants to Appspace that it will us the AI Features in accordance with all Laws.

Appspace represents and warrants to Customer that it will comply with all Laws in providing the AI Features, including but not limited to the EU AI Act Chapter II, Art 5.

2. OUTPUT

Customer acknowledges that the AI Features consist of emerging and evolving technologies, and as a result, the Output may contain results that are incorrect, biased, inaccurate. Customer shall be solely responsible for reviewing and evaluating the Output, and shall use the Output at its sole discretion and risk.

Customer acknowledges that the Output may not be unique, and the AI Features may generate similar or the same content for other Appspace customers. The Output may not be legally protectable under intellectual property laws in all jurisdictions. Customer's license and/or ownership rights in the Output, including any Appspace intellectual property included therein, shall be subject to Customer's ownership and license rights in the Subscription Services as described in the Agreement.

Appspace's indemnification obligations in Section 10.2 of the Agreement shall apply to the AI Features, but not to the Output.

3. ACCEPTABLE USE

In addition to Customer's compliance with Appspace's Acceptable Use Policy, Customer will use AI Features in accordance with the applicable Documentation, and will not use any AI Features or Output to:
(a) Promote or facilitate illegal activities or unlawful actions;

(b) Facilitate fraudulent actions;
(c) Attempt unauthorized access to any system, property, or information;
(d) Generate content that expresses or promotes hate, harassment, or violence, exploits or harms children, encourages self-harm, presents illegal, sexual, political, harmful, false, deceiving or misleading information, misuses personal data;
(e) Generate sexually explicit content;
(f) Distribute any ransomware, viruses, malware or spam;
(g) Generate any content that infringes, misappropriates or violates any third party rights; or
(h) Reverse engineer, disassemble, reverse compile, decompile, translate or otherwise attempt to discover the source code or underlying components of models, algorithms, and systems of the AI Features (except to the extent such restrictions are contrary the Law);
(i) Falsely impersonate an individual or mislead any individual that such content is human-generated.
(j) Develop, train, or improve other artificial intelligence services or artificial intelligence models
(k) Use web scraping, web harvesting, or web data extraction methods to extract data from the AI Features or Output

4. WARRANTY DISCLAIMER

IN ADDITION TO ANY DISCLAIMERS SET FORTH IN THE AGREEMENT, THE AI FEATURES AND OUTPUT ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. APPSPACE AND ITS THIRD-PARTY PROVIDERS, MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE OPERATION OF THE AI FEATURES, OR THE INFORMATION, TEXT, AND CONTENT INCLUDED IN THE OUTPUT, OR THE USE OF THE OUTPUT, INCLUDING WITHOUT LIMITATION, ACCURACY OF THE RESULTS, AVAILABILITY, SUITABILITY, RELIABILITY, OR CONTENT OF ANY INFORMATION PROVIDED THROUGH THE AI FEATURES. APPSPACE OR ITS THIRD-PARTY PROVIDERS WILL HAVE NO LIABILITY OR RESPONSIBILITY ARISING IN ANY WAY FROM THE USE OF THE AI FEATURES OR ANY ERRORS OR OMISSIONS CONTAINED IN THE OUTPUT, AND THE OUTPUT DOES NOT REPRESENT APPSPACE'S VIEWS.

Data Security Exhibit

Appspace Security Controls and Standards

Contents Table

Appspace Security Overview

Overview

The Appspace platform is a content management workplace experience solution provided to customers in a SaaS model. The platform requires customers to initiate access and interact with the platform through uploading relevant content, data and files to display on their internal network display devices or other devices in their corporate environment.

The following controls identifies security controls Appspace has in place to protect the Confidentiality, Integrity and Availability of customer data; but additionally identifies security controls customers are required to enforce on systems, files, users and data interfacing with the Appspace platform. These controls are referred to a “Complementary User Entity Controls”

Background

Appspace is currently SOC-2 Type II and ISO 27001:2022 compliant. We additionally have completed our CSA STAR Level 1 recognition; in addition to being Microsoft 365 certified the integration of our platform with specific Microsoft products.

Security Program

In order to maintain our ISO 27001:2022 certifications; we have built an Information Security Management Systems (ISMS) program across the organization. In addition to the ISO controls we adhere to; we additionally follow the NIST 800-53 Rev 4 guidelines to implement controls across our processes, people, systems and services. For additional information; please refer to the ISO/IEC 27001:2022 standard and the NIST 800-53 Rev 4 guidelines for a list of controls we adhere to under our security program. In 2024, Appspace will move to the new ISO 27001:2022 standard.

Appspace is audited by our third-party auditors as part of our security compliance program. For additional information, please refer to our Trust Page.

The controls listed in the security addendum are independently audited by a third party auditing firm to validate compliance across the ISO27xxx standards and SOC-2 Type 2.

Glossary of Terms

Term	Meaning
ISMS	Information Security Management System
Platform	Appspace Customer Environment.
Confidentiality	Protects sensitive information from unauthorized access. It's similar to privacy, and includes methods to protect personal privacy and proprietary information
Integrity	Ensures that data is accurate and unchanged throughout its lifecycle. It also ensures that data is authentic and non-repudiable.

Availability	Ensures that authorized users have reliable and timely access to information. It involves maintaining the hardware and systems that store and display information.
SAMM	Software Assurance Maturity Model
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
ASVS	Application Security Verification Standard

Appspace Information Security Controls and Standards

Control Objective	**Control Explanation**

Information Security Policies	Under the Appspace ISMS Program; Appspace has implemented a number of internal security policies to cover the security of the following areas: - People - Access Controls and Least Privileged Access - Systems Controls - These controls cover a broad range of policies and technical controls which are enforced. This will be be described through the document - Inherited Controls - These controls are controls provided to us by our sub-service cloud provider or physical controls passed to us for our offices. No production data resides within Appspace's offices. - Process Controls: These are controls documented in our Information Security policies which are in turn passed down to the appropriate technology teams to adhere to. - These policies and procedures contain confidential information and are only shared with our third-party auditors only. - These policies are stored in accessible locations for the appropriate employees. - All policies are reviewed twice per year. One review is completed prior to our required internal audit and another review is completed prior to our numerous third-party audits. - The following control objectives refer to a specific policy and procedure under the ISMS program. **Policies are not shared externally.**
Internal Organization Security	- All potential employees are required to successfully complete an employment, criminal and academic background check prior to commencing employment. - All new hire access is reviewed and approved based on their role and seniority. Appspace Security has the ability to deny the request for access to certain systems and create a custom role in order to adhere to our least privilege policy - Segregation of duties are enforced through both role-based access controls and least privileged access. An example would be software developers do not have access to make production changes. - All personnel employed by Appspace are required to use company owned devices where access is provisioned. If personal mobile devices are used then an MDM policy is enforced on the device. - Appspace security controls enable remote management of all devices connected to our systems.
Information Security in Program Management	- Appspace implements the Software Assurance Maturity Model as part of the development of our platform along with the STRIDE security model. In addition to these models, Appspace regularly performs internal penetration testing activities which

	map back to the ASVS standard to ensure we are securely developing, testing, remediating and maintaining the Confidentiality, Integrity and Availability of the platform
Mobile Devices and Teleworking	Ensuring the security of mobile devices and teleworking personnel This is managed through policy and MDM enforcement across all devices accessing internal systems. Mobile devices are not permitted to access customer cloud tenants.
Mobile Device Policy	This policy covers the management of employees' devices connecting to company internal assets. Mobile devices do not access customer tenant data.
Physical security	No customer data is stored or processed through our office locations. Appspace offices are provided as an in-office option for our remote workforce. All employees are provided badges to enter their local office and building management addresses physical security controls like visitor check-in, building security, cameras and fire/safety controls.
Human Resource Security	All prospective employees are required to validate their right to work in the region they are hired in. Their previous work and/or academic experience. If permitted to do so by the country of employment, background checks are performed.
Screening/Onboarding	Background checks are performed for new hires, acknowledging the company handbook, signing our confidentiality agreement and successfully completing the security awareness training program are required processes to complete an individual's onboarding responsibilities.
Terms and conditions of employment	This is handled through our confidentiality agreement, privacy policy and the company employee handbook
During Employment	During employment, employees are required to use company-owned devices to access internal systems. Employees are additionally required to review and sign the Appspace Internal Security Policy, the Appspace Employee Handbook and successfully complete their annual Security Awareness training. Employees in specific roles may be required to complete additional skill-based training like Privacy or OWASP Top 10 testing.
Management responsibilities	Appspace management requires all employees to undertake their assigned security awareness training on an annual basis. In addition, the Engineering teams undertake Secure Development education. The Appspace security team members are required to hold at least one security certification

Information security awareness, education and training	All new hires are required to successfully complete their security awareness training. On an annual basis, employees are required to successfully complete their security awareness training. In line with our ISO 27001 standards; all developers are required to successfully complete secure software development training (OWASP Top Ten). If applicable to their role and job function; employees are required to take additional privacy and other forms of training.
Disciplinary process	This process and policy is stated in the Appspace Employee handbook which all employees are required to review and agree to on an annual basis
Termination or change of employment responsibilities	As part of Appspace terms of employment and confidentiality agreement in the employee handbook, all ex-employees are required to return Appspace owned equipment which is tracked via an IT ticket and are required to keep Appspace information confidential. The IT ticket includes removing their access from all systems. 1) Access was removed or modified 2) Return company assets in the event of voluntary or involuntary leave.
Asset Management	Our internal asset management tracking system is reviewed on a regular basis and only admins have the ability to register assets.
Responsibility for assets	Appspace IT Admins are responsible for ensuring our asset management is kept up to date. An internal audit is performed on these systems and our external audits require us to demonstrate how these systems maintain their integrity and keep up to date.
Inventory of assets	Maintained through our asset management system.
Ownership of assets	All assets are company owned/managed. Only company-owned assets access customer data. Non-managed devices have restricted access due to our MDM policy
Acceptable use of assets	All employees are required to read and sign our Acceptable Use Policy within our Employee Handbook on an annual basis or upon hire.
Return of assets	Inventory of assets to demonstrate they were returned to Sean and Jameson documented it before it was reimaged
Information classification	Appspace has four levels of data classification where access to data is restricted through role-based access controls and DLP controls.
Classification of information	Part of the Data Classification Policy
Labeling of information	Managed by our DLP and Data Classification Policy

Handling of assets	Data Classification Policy and Data Labels restrict access and use of data depending on its classification level.
Management of removable media	This is blocked for users who do not require it.
Disposal of media	Google Cloud Data Destruction processes are used to securely delete customer data. This is inline with NIST SP 800-88 standards.
Access control	Access controls enforces logical and physical controls limiting access to information and resources based on an individual's role and responsibilities.
Business requirements of access control	All submitted IT tickets will include a business requirement and justification to permit an individual's access to data
User access management	Customize workflow and controls to management identity access management to data and systems.
User registration and de-registration	Managed through the internal Identity Management System
User access provisioning	Managed through the internal Identity Management System
Management of privileged access rights	Managed through the internal Identity Management System
Management of secret authentication information of users	Managed through the internal Identity Management System
Review of user access rights	Managed through the internal Identity Management System and reviewed on a quarterly basis.
Removal or adjustment of access rights	Managed through the internal Identity Management System and completed within 24 hours of a termination or an individual's departure.
User Responsibilities	Employee's responsibilities are noted in internal policies and procedures. This information is not available for external distribution.
Use of secret authentication information	Employee's responsibilities are noted in internal policies and procedures. This information is not available for external distribution.
System and application access control	Employee's responsibilities are noted in internal policies and procedures. This information is not available for external distribution.
Information access restriction	Managed and reviewed by both the Systems and Security teams

Secure log-on procedures	Managed and reviewed by both the Systems and Security teams
Password management system	Managed and reviewed by both the Systems and Security teams
Access control to program source code	Managed through the internal Identity Management System and reviewed on a quarterly basis.
Cryptography	Accepted industry practices are used for cryptographic methods and protocols.
Key management	A Key Management System is used to store sensitive information like certificates, cipher details and tokens as an example.
Physical and environmental security	Key cards and third-party building management services secure office locations. Customer data is not stored or processed in our office locations.
Change management	Change Management processes and approvals are in place prior to any data being promoted to production.
Separation of development, testing and operational environments	Separate networks for non-production and production environments. Non-production is segmented from customer environments.
Protection from Malware	A globally managed anti-malware software is managed by the security team on all company owned devices.
Backup	Customer data is backed up at least every 4 hours
Event logging	Security and Operational events are monitored and reviewed by our production support teams and security operation centers.
Protection of log information	Google protects the logs from deletion
Administrator and operator logs	Logging is enabled
Clock synchronization	Google manages UTC and Logging
Management of technical vulnerabilities	Appspace patches their production systems on a monthly basis. Security vulnerabilities identified with a CVSS of 9.0 or above is patched as soon as a vendor patch is made available.
Network controls	Firewall rules in GCP and overview of segregated networks. IPS configuration.
Security of network services	Security controls, business requirements for security controls and risk assessment. Encryption at rest, Encryption in transit and risk assessment plan

Agreements on information transfer	Defined in our Data Processing Addendum
Confidentiality or non-disclosure agreements	Appspace NDA and Confidentiality Agreements and https://www.appspace.com/legal/
Securing application services on public networks	Encrypts data in transit - TLS 1.2 and 1.3
Secure development policy	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
System change control procedures	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
Technical review of applications after operating platform changes	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
Restrictions on changes to software packages	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
Secure system engineering principles	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
Secure development environment	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
System security testing	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
System acceptance testing	Appspace leverages the Software Assurance Maturity Model for secure development and testing practices.
Production Data	Production Data is not used or copied to test or development environments.
Protection of Production Data	Production Data access is protected by a series of role-based access controls for privileged accounts. This is based on a “need to know” principle.
Information and communication technology supply chain	Security Controls - Suppliers SOC-3 or IS027001 reports is reflective of how well the infrastructure and services are maintained to support the ISMS system
Monitoring and review of supplier services	Annually review the suppliers security audit reports - SOC-3 report

Information security aspects of business continuity management	Appspace' business continuity plan is tested annually to ensure it meets our RTO and SLAs.
Management of information security incidents and improvements	Appspace tests its systems through an Incident Response Plan on an annual basis. All Lessons Learned and Action Items are completed within 90 days.
Reporting information security events	Upon discovery of an unauthorized access security event impacting customer data; Appspace will notify impacted parties within 72 hours upon discovery.
Reporting information security events	Communication is sent to Appspace personnel on a yearly basis to report potential security incidents, phishing events, suspicious emails or unauthorized access. The communication is sent to: Security@appspace.com
Verify, review and evaluate information security continuity	Appspace is audited on an annual basis by its third-party auditors to assure we have completed a Business Continuity Plan Test and a Disaster Recovery Test on an annual basis.
Identification of applicable legislation and contractual requirements	Appspace follows legal and regulatory framework as applicable to the platform
Privacy and protection of personally identifiable information	Appspace adheres and follows the General Data Protection Regulation standard along with the Data Privacy Framework standard
Regulation of cryptographic controls	Appspace stores all data in an encrypted format using AES-256 Data Encryption Keys
Independent review of information security	Appspace performs an annual SOC-2 Type II audit and Penetration Test . We have a roadmap of additional audits. We are independently audited by Microsoft as part of our Partner Certification standard.
Technical compliance review	Verify system consistency after a patch is applied or the instance is restarted.

Service Level Agreement

This Service Level Agreement (this "**SLA**") is incorporated into and made a part of the Appspace End User Agreement entered into by and between Appspace and Customer (the "**Agreement**"). All capitalized terms that are used but not defined in this SLA shall have the respective meanings given to them in the Agreement.

1. SUPPORT AND MAINTENANCE SERVICES

In the event there is an issue that affects Customer's ability to effectively access and use the Products (an "**Incident**"), it may contact Appspace, report the Incident, and request Appspace's help in resolving it. Committed response times for all Incidents are governed by the Product level purchased by Customer under the Agreement, as outlined in the table below. Appspace measures its response times in Business Hours, starting from the time of receipt by Appspace of the initial Incident report through Appspace's online support portal.

- Base (Free) = N/A
- Advanced = 12 hours (Subscription Services only)
- Premium = 4 hours (Subscription Services), 8 hours (Software)
- Elite = 2 hours (Subscription Services), 4 hours (Software)
- 24/7 = 1 hour (Subscription Services and Software)
- Strategic = 1 hour (Subscription Services and Software)

Appspace shall use commercially reasonable efforts to resolve any Incident promptly.

2. AVAILABILITY SERVICE LEVEL

During the term of the Agreement, Appspace shall ensure 99.9% System Availability over any calendar month. Should Appspace fail to achieve 99.9% System Availability over a calendar month, Customer shall have the right to receive, as an exclusive remedy for its breach of this obligation, the applicable service level credit ("**Service Level Credit**") set forth in Section 4 below.

3. DEFINITIONS

"Available" means the time periods that the Products are accessible by Customer.

"**Availability Failure**" has the meaning given the term in Section 4(a) below.

"Business Hours" means the hours of 8:00am – 5:00pm, Monday – Friday, in Customer's nearest Appspace regional office as indicated below. Business Hours do not include any local or regional holidays. Appspace's regional offices are as follows:

- Dallas — GMT -6 (CST)
- London – GMT 0 (or GMT +1 for BST)
- Dubai – GMT +4 (8:00am – 5:00pm, Sunday – Thursday)
- Kuala Lumpur – GMT +8

"Emergency Maintenance" means maintenance may be required to address material security-related issues or technical problems that would impact the availability of the Products and resolution of which cannot wait until the next Scheduled Maintenance or cannot be remedied in the course of Scheduled Maintenance. Appspace shall use commercially reasonable efforts to notify Customer in advance of any Emergency Maintenance, and shall promptly notify Customer of the Emergency Maintenance and actions being taken in the course thereof once Appspace becomes aware of an occasion requiring Emergency Maintenance.

"Force Majeure Event" means an event beyond either party's reasonable control (excluding payment obligations under the Agreement), including without limitation, significant failure of a part of the power grid, sabotage, denial of service attack, significant failure of the Internet, natural disaster, war, riot, insurrection, pandemic, epidemic, strikes or other organized labor action, terrorism, or other events of an unforeseeable nature. The Party affected by the Force Majeure Event shall diligently attempt to remove such cause or causes and shall promptly notify the other Party of the existence of the Force Majeure Event and its probable duration.

"Scheduled Maintenance" means maintenance performed by or on behalf of Appspace for which Appspace provides notice to Customer of such maintenance no less than 72 hours prior to the occurrence of maintenance that will involve both Parties. "Scheduled Maintenance" shall not include instances of Emergency Maintenance unless otherwise agreed by the Parties in writing.

"Scheduled Uptime Minutes" means the difference between (a) the total aggregate minutes in the applicable month and (b) minutes in that month in which the Products are not Available to Customer due to Scheduled Maintenance.

"**System Availability**" means the percentage of total time during which the Products are Available to Customer.

"Unscheduled Outage Minutes" means all those minutes in which the Products are not Available to Customer, excluding minutes arising from any of the reasons specified in Section 4(c) below. Unscheduled Outage Minutes shall be counted from the time that Customer notifies Appspace of an outage to the time that a representative of Appspace notifies Customer that the outage is resolved.

4. SERVICE LEVEL CREDITS

a. Service Levels. In the event the System Availability of the Products are less than 99.9% over a calendar month (an "**Availability Failure**"), Customer shall be eligible for a credit for the calendar month's portion of the Products fees in the amounts set forth below, prorated accordingly in the event of an annual or quarterly Products fees.

System Availability will be expressed as a percentage calculated in accordance with the following formula:

$$\text{System Availability \%} = \frac{(\text{Scheduled Uptime Minutes} - \text{Unscheduled Outage Minutes})}{\text{Scheduled Uptime Minutes}}$$

b. Service Level Credits. In the event that Appspace fails to meet the System Availability objectives set forth above, Customer will be entitled to a Service Level Credit of 1% of the fees paid or payable for the

Products during each calendar month for every 1% by which the System Availability is less than 99.9% of time for said month, provided such Service Level Credit shall not exceed 25% in any calendar month. Appspace will notify Customer within thirty (30) days if Customer is eligible for a Service Level Credit from the prior calendar month. At Appspace's option, the Service Level Credit will either be (a) set off against any fees or other charges payable to Appspace under the applicable Order, or (b) payable to Customer via check or ACH.

c. Exceptions. Notwithstanding anything herein to the contrary, minutes in which the Products are not Available due to any of the following reasons shall not be considered Unscheduled Outage Minutes or a failure to meet the System Availability commitment for the purposes of the calculation of System Availability:

i. Failure of hardware, software or other equipment not provided by Appspace and used by Customer in connection with the Products;
ii. Customer's inability to access its internet service provider via Customer's internal network gateway, or Customer's internet service provider's inability to access the Products due to technical difficulties of Customer's internet service provider;
iii. Scheduled Maintenance;
iv. Force Majeure Event suffered by Appspace;
v. Customer not providing information or approval that is necessary to bring the Products back online;
vi. Mutually agreed upon unscheduled maintenance which remediates a critical priority problem;
vii. Failures due to catastrophic outages suffered by Appspace's hosting provider;
viii. A suspension of Customer s access to Products due to the reasons described in the Agreement; and
ix. Emergency Maintenance.

Data Processing Addendum

This Data Processing Addendum (this "**Addendum**") forms part of the Appspace End User License Agreement (the "**Agreement**") between you ("**you**" or "**Customer**") and Appspace, Inc. a corporation formed under the laws of the state of Delaware, with offices located at 400 N. Tampa St., Suite 1725, Tampa, FL 33602, USA ("**Appspace**") for the provision of the Products. Capitalized terms not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Appendices conflicts with the Agreement, this Addendum shall take precedence. The term of this Addendum corresponds to the duration of the Agreement.

1. Definitions

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Data Protection Legislation" means all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable, the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq., ("CCPA"), as well as any guidance notes and codes of practice issued by the European Commission, European Data Protection Board and applicable national supervisory authorities including without limitation the UK Data Protection Act 2018, UK GDPR, GDPR and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426), Swiss Data Protection Act 2020 and all local or national laws and regulations implementing the aforementioned, in each case as may be updated, amended, supplemented or replaced from time to time.

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

"Customer Personal Data" means the Personal Data within Customer Data Processed by Appspace on Customer's behalf in the course of providing Products to Customer.

"GDPR" means EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data.

"International Data Transfer" means any transfer of Customer Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom.

"Personal Data" shall have the meaning assigned to the terms "personal data" or "personal information" under applicable Data Protection Legislation.

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

"**Personal Data Breach**" means the actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

"**Standard Contractual Clauses"** means (i) where the GDPR applies, the standard contractual clauses adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021 (the "**EU/EEA SCCs**"); (ii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized

by the Swiss Federal Data Protection and Information Commissioner (the "**Swiss SCCs**"); and (iii) where UK Data Protection Law apply, the standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR (the "**UK SCCs**").

"**Subprocessor**" means Appspace's authorized Affiliates, vendors and third-party service providers that Process Customer Personal Data in the course of providing the Products.

"UK Addendum" means the addendum to the Standard Contractual Clauses issued by the UK information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).

"UK GDPR" means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018.

"**Data Controller**", "**Data Processor**", "**Business**", and "**Service Provider**", shall be interpreted in accordance with applicable Data Protection Legislation.

2. DATA PROTECTION

2.1 Roles of the Parties. The provisions of this Section 2 shall apply to the Processing by Appspace of Customer Personal Data in the course of providing Customer the Products, as detailed in Appendix 1A of this Addendum. Customer is the Data Controller and/or Business and Appspace is the Data Processor and/or Service Provider in relation to Customer Personal Data.

2.2 Processing Instructions. Appspace will Process the Customer Personal Data only in accordance with Customer's documented instructions as set forth in this Addendum and the Agreement or as directed and documented by Customer through the Products, and in accordance with the requirements of Article 28(3) of GDPR. If Data Protection Legislation requires Appspace to Process the Customer Personal Data for any other purpose, Appspace will notify Customer of this requirement before processing, unless such law(s) prohibit the giving of notice on important grounds of public interest. Appspace will notify Customer promptly if, in Appspace's opinion, an instruction for the Processing of Customer Personal Data given by Customer violates applicable Data Protection Legislation.

2.3 Assistance under Data Protection Legislation. Where Appspace processes the Customer Personal Data under or in connection with the performance of its obligations under the Agreement, Appspace shall:

2.3.1 implement appropriate technical and organizational measures necessary to meet the requirements of Article 32 of the GDPR;

2.3.2 taking into account the nature of the Processing and the information available to Appspace, reasonably assist Customer to fulfil Customer's obligations under Data Protection Legislation:

(i) where possible, to respond to requests from Customers concerning Data Subjects exercising their rights in Customer Personal Data under Data Protection Legislation (e.g., access, rectification, erasure, data portability, etc.). If a request is sent directly to Appspace, Appspace will inform the requester to contact the Customer which is responsible for their Personal Data and will not otherwise respond to the request. In the event Appspace is unable to delete Customer Personal Data for reasons permitted under the Data Protection Legislation, Appspace shall (a) promptly inform Customer of the reason(s) for its inability to fulfill the deletion request, (b) ensure the continued privacy, confidentiality and security of such Customer Personal Data, and (c) delete the Customer Personal Data promptly after the reason(s) for Appspace's

inability to delete such data has expired

(ii) with respect to Articles 32 to 36 of the GDPR.

If changes in Data Protection Legislation result in new material obligations as it relates to Appspace's assistance under this Section 2.3.2, the Parties will work together in good faith to agree upon an acceptable resolution. Each Party shall be responsible for its own costs incurred under this Section 2.3.2; and

2.3.3 make available to Customer all information reasonably requested by Customer for the purpose of demonstrating that Customer's obligations relating to the appointment of Data Processors as set out in Article 28 of the GDPR have been met.

2.4 Information Security. In accordance with Appendix 1B, Appspace will implement and maintain commercially reasonable technical, administrative, and physical security measures designed to protect the Customer Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful Processing, accidental loss, destruction, damage or theft of Customer Personal Data and appropriate to the nature of the Customer Personal Data which is to be protected. In an effort to improve Appspace's overall security, Appspace may amend its security measures, provided that the new or replacement measures do not reduce the level of security provided by the existing measures. Notwithstanding the foregoing, such safeguards shall, at a minimum, be no less rigorous than accepted industry practices for information security or other applicable industry standards.

2.5 Personal Data Breach. Upon discovering or otherwise becoming aware of a Personal Data Breach, Appspace will notify Customer without undue delay (but no more than seventy-two (72) hours). Such notification shall not be interpreted or construed as an admission of fault or liability by Appspace.

2.6 Appspace's Subprocessors. Customer specifically authorizes the engagement of Appspace's Affiliates as Subprocessors. In addition, to the extent necessary to fulfill Appspace's contractual obligations under the Agreement and subject to Appspace's compliance with this Section 2.6, Customer generally authorizes Appspace to engage other Subprocessors, as described in Appendix 1A, whose Processing activities shall occur in Belgium.

2.6.1 When engaging any Subprocessor, Appspace ensures that:

(i) the Subprocessor only processes Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this Addendum);

(ii) data protection obligations consistent with those described in this Addendum are imposed on the Subprocessor through a written agreement; and

(iii) Appspace remains fully liable to Customer where the Subprocessor fails to fulfil its data protection obligations under the Agreement.

2.6.2 Prior to engaging any new Subprocessor, Appspace will, at least ten (10) days before the new Subprocessor Processes any Customer Personal Data, inform Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) in accordance with applicable Data Protection Legislation.

2.6.3 Customer may object to Appspace's use of a new Subprocessor by notifying Appspace within ten (10) days after notice has been given with Customer's grounds

for its objection. In the event Customer objects to a new Subprocessor, as permitted in the preceding sentence, Appspace will use commercially reasonable efforts to make available to Customer a change in the Products or recommend a commercially reasonable change to Customer's configuration or use of the Products to avoid Processing of Customer Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If Appspace is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either Party may terminate without penalty the applicable Order with respect only to those Products which cannot be provided by Appspace without the use of the objected-to new Subprocessor by providing written notice. Appspace will refund Customer any prepaid, unused fees covering the remainder of the term of such applicable Order following the effective date of termination with respect to such terminated Products, without imposing a penalty on Customer for such termination.

2.7 Confidentiality. Appspace will ensure that Appspace's personnel with access to the Customer Personal Data are subject to a binding duty of confidentiality with regard to such Customer Personal Data. Except as set forth in Section 2.6 above or in accordance with documented instructions from Customer (as set forth in this Addendum or the Agreement or as directed by Customer through the Products), Appspace will ensure that none of Appspace's personnel publish, disclose or divulge any Customer Personal Data to any third party.

2.8 Selling of Customer Personal Data Prohibited. The Customer Personal Data that Customer discloses to Appspace is provided to Appspace for a Business Purpose, as defined under the CCPA, and nothing about the Agreement or the Services involves the "selling" or a "sale" of Customer Personal Data under Cal. Civ. Code § 1798.140(t)(1).

2.9 Deletion or Return of Customer Personal Data. Appspace shall retain Customer Personal Data for the term of the Agreement provided that such retention does not conflict with a Data Subject request made pursuant to Section 2.3.1. Upon expiration or termination of the Agreement and upon Customer's written request, Appspace will securely destroy or return to Customer in a format of Appspace's choosing all Customer Personal Data, and destroy existing copies. Notwithstanding the foregoing, Appspace may retain copies of the Customer Personal Data disclosed hereunder that are contained in routine system backups or are necessary to fulfill its ongoing obligations or exercise its ongoing rights hereunder, subject to the ongoing obligation to maintain the confidentiality of such information in accordance with the terms the Agreement and this Addendum.

2.10 Audits. Appspace is regularly audited by independent third-party auditors and internal auditors to test and verify the security controls of Appspace and its people. Upon request and provided that the Parties have an applicable non-disclosure agreement in place, Appspace will allow Customer and Customer's authorized representatives to access and review up-to-date attestations, reports (e.g. external auditors) or suitable certifications to ensure compliance with the terms of this Addendum. Notwithstanding the foregoing, any review of aforementioned materials or audit must be conducted during Appspace's regular business hours, with reasonable advance notice to Appspace and subject to reasonable confidentiality procedures. In addition, reviews and/or audits shall be limited to once per year, unless (a) Appspace has experienced a Personal Data Breach within the prior twelve (12) months; (b) an audit is carried out at the direction of a government entity; or (c) an audit reveals a material noncompliance. Appspace shall be entitled to charge Customer a reasonable fee for any Appspace effort or costs in complying with this Section 2.10.

2.11 Data Protection Officer. The contact details for the team responsible for data protection at Appspace are: Sam.Baxter@appspace.com

2.12 European Economic Area Data Transfers. Upon separate, prior written approval from Customer, Appspace and its Subprocessors will be authorized to transfer Customer Personal

Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States. If Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Appspace in a country that has not been found to provide an adequate level of protection under Data Protection Legislation, the Parties agree to execute the EU/EEA SCCs and any necessary amendment to this DPA, but to the extent that and for so long as the EU/EEA SCCs cannot be relied on for a lawful transfer in compliance with the UK Data Protection Law or the Swiss DPA, the Parties agree to execute the UK SCCs or Swiss SCCS (or such applicable, superseding standard contractual clauses).

2.13 Compliance with UK Addendum. Customer and Appspace acknowledge and agree the UK Addendum will hereby be incorporated and apply to International Data Transfers out of the UK. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Customer and the "Importer" is Appspace, and their details are set forth in this section and the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the Module 2 Standard Contractual Clauses; (iii) in Table 3, Annexes 1 (A and B) & III, and II to the "Approved EU SCCs" are found in Appendix 1A and Appendix 1B respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

2.14 Compliance with Data Protection Legislation. Each Party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the Processing of Customer Personal Data and the performance of the Agreement and this Addendum, including without limitation, compliance with Article 31 of GDPR. With respect to Customer Personal Data, Customer as the Data Controller, is responsible the administration and management of Customer Personal Data, in addition to, obtaining, and demonstrating evidence that is has obtained all authorizations, lawful bases, and consents necessary for Appspace to Process Customer Personal Data in accordance with the Agreement and this Addendum.

2.15 Data Subject Requests. Customer is responsible for communications and efforts to comply with requests made by Data Subjects under the Data Protection Legislation. If any such request requires Appspace assistance, Customer shall notify Appspace of the Data Subject request in a reasonable amount of time and sent to privacy@appspace.com.

2.16 Limitation on Disclosure of Customer Personal Data. To the extent legally permitted, Appspace shall: (i) promptly notify Customer in writing upon receipt of an order, demand, or document purporting to request, demand or compel the production of Customer Personal Data to any third party, including, but not limited to the United States government for surveillance and/or other purposes; and (ii) to the extent possible, provide at least seventy-two (72) hours' notice prior to disclosing Customer Personal Data to any third party without providing Customer, so that Customer may, at its own expense, exercise such rights as it may have under applicable laws to prevent or limit such disclosure.

3. Customer Obligations

3.1 Customer shall continue at all times to have in place recognized lawful legal bases under Data Protection Legislation and all necessary data privacy notices to ensure that all processing of personal data by the Processor and all Subprocessors that is contemplated by this Addendum will be lawful and shall not contravene the obligations of a data controller under Data Protection Legislation.

4. Miscellaneous

4.1 Save as specifically modified and amended in this Addendum, all of the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern this Addendum. Except as otherwise expressly provided herein, no supplement, modification, or amendment of this Addendum

will be binding, unless executed in writing by a duly authorized representative of each Party to this Addendum. If any provision of the Addendum is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of this Addendum shall remain operative and binding on the Parties.

	APPSPACE
Customer's Full Legal Name	
Signature	Signature
Printed Name	Printed Name
Title:	Title:
_____	_____
Date:	Date:
_____	_____

Appendix 1A

Details of Personal Data Processing

This summary sets out details of the processing of Customer Personal Data under the Agreement by Appspace and any authorized Subprocessors (as listed below):

The subject matter and duration of the Processing	**SYSTEMS:** Appspace workplace experience hosted platform **SUBJECT MATTER**: The subject-matter of the Processing is the provision of the Products that involves the Processing of Customer Personal Data. **DURATION OF PROCESSING**: The Processing will be carried out until the Agreement terminates.
The nature and purpose of the Processing	**PURPOSES OF PROCESSING**: In accordance GDPR Art. 6, the lawful processing of information will be conducted to meet the performance of the contract (EULA) **LEGAL BASIS FOR PROCESSING**: EU and EEA organizations agree the legal basis for collecting, using and processing personal data as described below is in order for their users to experience the full benefits of the Appspace platform in accordance with Appspace's EULA **NATURE OF PROCESSING**: As part of our data minimization practices, the collection, storage and other Processing necessary to provide, maintain, and optimize the Products provided to Customer in accordance with the Agreement.
The types of Personal Data being Processed	**PERSONAL DATA**: ● Data Subject - Direct identifying information (e.g., first name, last name, and email address,). ● Indirect identifying information (e.g., job title, telephone number) ● Device identification and traffic data (e.g., Geolocation, IP addresses, cookies). **SPECIAL CATEGORIES OF PERSONAL DATA**: Appspace does not knowingly collect (and Customer shall not submit or upload) any special categories of data as defined under the Data Protection Legislation.

The categories of Data Subject	Customer and Affiliates employees and/or users.

Approved Subprocessors of Personal Data are:

#	Name	Territory	Area of use
1	Google LLC	Iowa, United States	*Cloud Hosting Services*
2	Google LLC	St. Ghislain, Belgium	*Cloud Hosting Services*
3	Google LLC	London, United Kingdom	*Cloud Hosting Services*
4	Google LLC	South Carolina, United States	*Cloud Hosting Services*
5	Google LLC	Oregon, United States	*Cloud Hosting Services*
6	Google LLC	Quebec, Canada	*Cloud Hosting Services*
7	Microsoft, Inc.	Iowa, United States	*Cloud Hosting Services*
8	Microsoft, Inc.	New South Wales, Australia	*Cloud Hosting Services*
9	Microsoft, Inc.	Paris, France	*Cloud Hosting Services*
10	Salesforce, Inc.	California, United States	*CRM/Support Services*
11	Gainsight, Inc.	California, United States	*CRM/Support Services*
12	SupportLogic, Inc.	California, United States	*CRM/Support Services*
13	Intercom, Inc.	California, United States	*CRM/Support Services*

Appendix 1B

Processor and Sub-Processor Internal Security Measures

Confidentiality (Article 32(1)(b) GDPR)

1. **Access control to premises and facilities**
   Measures must be taken to prevent unauthorized physical access to premises and facilities holding Customer Personal Data. Measures shall include:

   - Access control system
   - ID reader, magnetic card, chip card
   - (Issue of) keys
   - Door locking (electric door openers etc.)
   - Surveillance facilities
   - Alarm system, video/CCTV monitor
   - Logging of facility exits/entries

2. **Access control to systems**
   Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

   - Password procedures (incl. special characters, minimum length, forced change of password)
   - Hashing, Encryption and Cryptography measures
   - No access for guest users or anonymous accounts
   - Central management of system access
   - Access to IT systems subject to approval from HR management and IT system administrators

3. **Access control to data**
   Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized input, reading, copying, removal modification or disclosure of data. These measures shall include:

   - Differentiated access rights
   - Access rights defined according to duties
   - Automated log of user access via IT systems
   - Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

Integrity (Article 32(1)(b) GDPR)

1. **Disclosure control**
   Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

   - Compulsory use of encrypted private networks for all data transfers
   - Creating an audit trail of all data transfers

2. **Input control**

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained. Measures should include:

- Logging user activities on IT systems
- That it is possible to verify and establish to which bodies Customer Personal Data have been or may be transmitted or made available using data communication equipment
- That it is possible to verify and establish which Customer Personal Data have been input into automated data-processing systems and when and by whom the data have been input;

3. **Job control**
   Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

   - Unambiguous wording of contractual instructions
   - Monitoring of contract performance

Availability and Resilience (article 32(1)(b))

1. **Availability control**
   Measures should be put in place designed to ensure that data are protected against accidental destruction or loss. These measures must include:

   - Installed systems may, in the case of interruption, be restored
   - Systems are functioning, and that faults are reported
   - Stored Customer Personal Data cannot be corrupted by means of a malfunctioning of the system
   - Uninterruptible power supply (UPS)
   - Business Continuity procedures
   - Remote storage
   - Antivirus/firewall systems

2. **Segregation control**
   Measures should be put in place to allow data collected for different purposes to be processed separately. These measures should include:

   - Restriction of access to data stored for different purposes according to staff duties.
   - Segregation of business IT systems
   - Segregation of IT testing and production environments