

MASTER SOFTWARE LICENSE AND SUBSCRIPTION AGREEMENT

This Master Software License and Subscription Agreement (the “**Agreement**”) is made by and between AvePoint Public Sector, Inc., a Virginia Corporation, with offices at 2101 Wilson Boulevard, Suite 820, Arlington, Virginia 22201, (“AvePoint”) including if and where applicable its Affiliates (as defined below), and your company or entity Customer (“**Customer**”), for use of certain of AvePoint’s Services and/or Products (“**Solutions**”). Each party hereto shall be referred to as “**Party**”; collectively, the “**Parties**”. The Agreement consists of the terms and conditions set forth below, any exhibits, addenda, or appendices identified below, and any Order Forms that properly incorporate this Agreement as controlling. This Agreement is effective immediately upon execution of an Order (as defined below) (the “**Effective Date**”).

To the extent that there exists a previously negotiated Master Software License and Subscription Agreement or similarly negotiated license and/or subscription agreement between the Parties that is currently in effect at the time of this Agreement’s Effective Date (“**Prior Negotiated Agreement**”), the provisions of any such Prior Negotiated Agreement shall control unless expressly provided otherwise in such other agreements. In the event that there is no such Prior Negotiated Agreement, then the provision of the Solutions by AvePoint, and Customer’s use thereof, shall be governed by this Agreement.

Subject to the terms of this Agreement, AvePoint’s Solutions shall be provided to Customer as either web-based access to software as a service (“**SaaS Solution**”) or pursuant to a license to use AvePoint’s Software in Customer’s self-hosted environment (“**Licensed Solution**”). AvePoint reserves the right to update, enhance, or otherwise change the Solutions from time to time and may do so without Customer’s consent or agreement. AvePoint Solutions are limited in accordance with AvePoint’s licensing and access models as set out in this Agreement and updated periodically under

https://avepointcdn.azureedge.net/pdfs/en/AvePoint_Licensing_Access_Models.pdf. Solutions are deemed accepted upon being made available to Customer and are subject to no further or additional acceptance procedures. In consideration of the foregoing and of the mutual promises contained herein, AvePoint and Customer agree as follows:

1. AVEPOINT SOLUTIONS

1.1. SaaS Solutions. Customer may access and use the purchased SaaS Solutions on a Subscription basis solely for its internal business operations and purposes, subject to this Agreement, the Documentation, and any scope of use restrictions and Solution descriptions on the applicable Order. A SaaS Solution is limited for the time period specified in the Order as follows: (a) access per user: one user per time period in accordance with the fees set forth on the Order; or (b) access per usage: access is based on the number, size or amount of data processed by the SaaS Solution and is limited to the amount specified on the Order. Acceptance of the Solutions is neither contingent upon the delivery of any future functionality or features, nor is it dependent upon any oral or written public comments made by AvePoint with respect to future functionality or features. Customer is responsible for use of the SaaS Solution by its Authorized Users (as defined below) and their full compliance with this Agreement. Customer shall keep confidential its user IDs and passwords and remain responsible for all actions taken through its accounts.

1.1.1. SaaS Service Level Agreement. SaaS Solutions shall have an uptime of not less than 99.9% (resulting in a Downtime of more than 43 minutes and 49 seconds) per month (“**SLA**”). AvePoint must receive sufficiently detailed excessive Downtime claims no later than the end of the calendar month following the month in which the alleged Downtime occurred. Should the Parties determine that AvePoint has not met the uptime requirement following AvePoint’s investigation, Customer shall be entitled, as an exclusive remedy, to a Service Credit not to exceed in any particular month, fifteen (15%) of the monthly fees. Notwithstanding the foregoing, if the Parties determine that the SaaS

Solution(s) had an uptime of less than ninety-nine percent (99.0%) (resulting in a Downtime of more than 7 hours and 18 minutes) in a specific month, Customer shall be entitled, as an exclusive remedy, to a Service Credit of twenty percent (20%) of the fees applicable for that specific month. If Customer purchased a SaaS Solution from a Partner, the Service Credit will be based on the estimated retail price for the applicable SaaS Solution, as determined by AvePoint in its sole but reasonable discretion. Service Credits shall be credited to Customer within thirty (30) days of the excessive Downtime determination.

1.1.2. SaaS Exclusions. AvePoint shall use commercially reasonable efforts to make the SaaS Solutions available at the gateway between the public internet and the network of the Cloud Services Provider, except for: (i) scheduled Downtime (of which AvePoint shall, to the extent practicable, schedule so as not to adversely affect Customer's business); and (ii) as set forth in the Agreement. AvePoint shall use reasonable efforts to give ten (10) days' notice of any service maintenance to the infrastructure network, hardware, or software used by AvePoint if AvePoint, in its reasonable judgment, believes that such maintenance will impact Customer's use of its production instances. Notwithstanding the foregoing, no notice may be provided if AvePoint, in its sole and reasonable discretion, determines that maintenance is needed to secure the availability, security, stability, or performance of the SaaS Solution. Uptime and Downtime, and any additional performance targets, shall not apply to the extent performance or availability issues result from scheduled Downtime or are directly or indirectly due to factors beyond AvePoint's reasonable control, including but not limited to those that are (i) caused by a fault, failure, or availability of the internet or any public telecommunications network; (ii) caused by a fault, failure, or availability problems of the Cloud Storage Provider; (iii) caused by a fault, failure, or availability problems of any cloud-based services registered by Customer in the SaaS Solution; (iv) caused by Customer's hardware or software; (v) caused by the actions or inactions of Customer; (vi) caused by Customer's use of the SaaS Solution other than in accordance with the Agreement; or (vii) attributable to the acts or omissions of Customer or Customer's Authorized Users, or anyone gaining access to the

SaaS Solution by means of Customer's Accounts, passwords, or equipment.

1.1.3. Additional SaaS Performance Targets. AvePoint, in its sole discretion, may announce additional performance targets for SaaS Solutions and shall use commercially reasonable efforts to meet such targets. Nonetheless, the Parties agree that failure to meet such additional performance targets shall not entitle Customer to a refund of any fees paid under the Agreement.

1.1.4. Suspension of SaaS Solutions. Customer is responsible for all activities conducted by it or through the accounts of its Users of the SaaS Solution. Without limiting AvePoint's termination or other rights, AvePoint reserves the right in its sole but reasonable discretion to temporarily suspend Customer's access to the SaaS Solutions (and any related services) in whole or in part (a)reserved; (b)for Customer's breach of Section 1.4 (Use Restrictions or Section 1.2 (Licensed Solutions; Limitations); or (c) to prevent harm to other customers or third parties, or to preserve the security, availability, or integrity of the SaaS Solutions. When practicable, AvePoint will use reasonable efforts to provide Customer with advance notice in accordance with Section 12.4 (Notices). Unless this Agreement has been terminated, AvePoint will cooperate to restore Customer's access to the SaaS Solutions promptly after AvePoint has verified that Customer has resolved the issue causing suspension.

1.2. Licensed Solution; Limitations. If Customer has purchased a Licensed Solution, subject to this Agreement, AvePoint grants to Customer, and Customer agrees to pay for, a non-exclusive, non-transferable license to use the Licensed Solution. This license grant is solely for Customer's Internal Use in accordance with this Agreement and the terms set forth on the applicable Documentation delivered with the Software. Except as expressly provided elsewhere in this Agreement, no sublicensing of use or access is permitted for any Solutions. The preceding sentence notwithstanding, and except as otherwise agreed between the Parties, Customer may distribute or deploy (but not sublicense) the Licensed Solution(s) to its Affiliates for use solely by the maximum number of Authorized Users or licensed quantities set forth in the Order.

Except as expressly set forth in this Agreement, no license is granted and none shall be deemed granted, by implication, estoppel, or otherwise.

1.2.1. Types of Licenses.

1.2.1.1. Term Licenses. A Licensed Solution is limited for the time period specified in the Order as follows: (a) Licensed per user: one License per user per time period in accordance with the fees set forth on the Order; (b) Licensed per Named Domain: one License per specific domain name ("**Named Domain**") as set forth on the Order; (c) Licensed per usage: the License granted hereunder is based on the number, size or amount of data processed by the Licensed Solution and is limited to the amount specified on the Order; and/or (d) Licensed per Locality: one License per locality as defined in the Order.

1.2.1.2. Perpetual Licenses. A Licensed Solution that is offered under a Perpetual License may be further limited by the Order as follows: (a) Licensed per SharePoint Server: one Perpetual License per SharePoint Server that is being administered through the Licensed Solution; (b) Licensed per usage: the Perpetual License granted hereunder is based on the number, size or amount of data processed by the Licensed Solution and is limited to the amount specified on the applicable Order; (c) Licensed per Named Domain (if offered by AvePoint under a perpetual license model): one Perpetual License per Named Domain as set forth on the applicable Order; and (d) for a Licensed Solution that is classified as part of the DocAve Software Platform, one Perpetual License per DocAve Manager and per Media Services used, where such usage is limited to the amount specified on the applicable Order.

1.3. Excess Usage. During the Term, in the event Customer requests or requires additional quantities of the granted Subscriptions or exceeds the allotted quantities of the granted Subscriptions indicated on the applicable Order ("**Excess Usage**"), AvePoint will invoice Customer, and Customer shall be responsible for payment to AvePoint, for such Excess Usage. The price shall be the then-current price per unit (excluding any discounts) of the Subscriptions and the duration of Excess Usage, unless the Parties otherwise agree in writing. For avoidance of doubt, all additional Subscriptions

purchased for Excess Usage shall align with the Subscription Term defined in the initial Order.

1.4. Use Restrictions. Customer shall not (and shall not permit any third party to): (a) license, sub-license, sell, re-sell, rent, lease, transfer, distribute, provide access to or otherwise make available any Solutions to any third party except as provided for expressly in this Agreement or in an Order; (b) use the Solutions to provide or incorporate the Solutions into any product or service provided to a third party; (c) use the Solutions to develop a similar or competing product or service; (d) reverse engineer, decompile, disassemble, modify, or otherwise seek to obtain the source code or non-public APIs to the Solutions, except to the extent expressly permitted by applicable law (and then only upon advance Notice to AvePoint); (e) copy, modify or create any derivative work of the Solutions or any Documentation; (f) remove or obscure any proprietary or other notices contained in the Solutions (including any reports or data printed from the Solutions); (g) publicly disseminate performance information regarding the Solutions; (h) use the Solutions to create, use, send, store or run viruses or other harmful computer code, files, scripts, agents or other programs or engage in any other malicious act; (i) disrupt their security, integrity or operation; (j) remove or modify a copyright or other proprietary rights notice in the Solutions; (k) use the Solutions to reproduce, distribute, display, transmit or use material protected by copyright or other intellectual property right (including the rights of publicity or privacy) without first obtaining the permission of the owner; (l) use them unlawfully or in any manner which violates any applicable law or regulation; or (m) use them in a manner that temporarily or permanently alters, erases, removes, copies, modifies, halts or disables any AvePoint or third party data, software or network. Customer must not permit any unauthorized person to access or use the Solutions and shall use reasonable endeavors, including reasonable security measures relating to Account access details, to ensure that no unauthorized person may gain access to the Solutions using an Account. Customer shall be responsible for the lawfulness of, and results obtained from, all Customer Data submitted by users and each user's acts and omissions.

1.5. User Compliance Check. AvePoint may, with reasonable notice and at any time during reasonable business hours, not more than once every twelve months, either on its own or through its duly authorized representative, conduct a review of the Customer's compliance with the terms of this Agreement (including but not limited to Customer's use of the Solutions). Notwithstanding the foregoing, AvePoint may use technical measures to conduct compliance checks on an ongoing basis to determine if there is Excess Usage as set out in Section 1.3 above.

2. DATA PRIVACY

2.1. Security. AvePoint shall use commercially reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration, or disclosure of the Solutions or Customer Data, as further described in AvePoint's then-current DPIS Policy.

2.2. Customer Data. All Personal Data received or collected by AvePoint in connection with the performance of this Agreement (including its amendments) will be processed in accordance with AvePoint's Privacy Policy, which can be accessed at <http://www.avepoint.com/company/privacy-policy>, attached hereto, as non-materially amended from time to time. Any Personal Data received or collected by AvePoint or its Affiliates will further be processed in accordance with applicable data protection laws. Where the Personal Data is that of a third party, Customer certifies that it has obtained that data pursuant to applicable data protection laws and has obtained all necessary authorizations and consents with respect to such information. AvePoint shall maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data and Business Contact Information, including, but not limited to measures for preventing access, use, modification or disclosure of Customer Data or Business Contact Information except (a) to provide the SaaS Solutions and prevent or address service or technical problems; (b) as compelled by law; or (c) as expressly permitted by Customer in writing. Such specific safeguards shall be as set forth in the Documentation. When providing Customer Data or Business Contact Information, Customer shall not under any circumstances provide Personal Data to AvePoint for

the processing of such data on behalf of Customer, as defined in Article 28.1 GDPR, unless agreed otherwise by way of a separate written agreement between the Parties. All Customer Data passing through SaaS Solutions is stored by AvePoint in a Customer-selected data center. If there is a geographic region indicated on the applicable Order or the website where Customer registers for the SaaS Solutions, Customer Data and all operations will reside and execute from that geographic region's data center, save for (temporary) emergency purposes. Customer acknowledges and to the extent necessary approves that information provided to AvePoint (other than Customer Data) may be stored and processed by AvePoint in the United States or in other countries.

2.3. Rights in Customer Data. Customer is solely responsible for the accuracy, content, and legality of all Customer Data. Customer represents and warrants to AvePoint that (1) Customer will comply with all applicable laws in its use of the Solutions (including but not limited to, if applicable, the California Online Privacy Protection Act, GDPR and similar laws governing the protection of personal data) and (2) Customer has provided all disclosures and obtained all necessary rights, consents and permissions to collect, share and use Customer Data as contemplated in this Agreement (including granting AvePoint the rights herein) without violation or infringement of (i) any third party intellectual property, publicity, privacy or other rights, (ii) any Laws, or (iii) any terms of service, privacy policies or other agreement governing Customer Properties or Customer's accounts with third-parties. Customer grants to AvePoint and its Affiliates a non-exclusive, worldwide, limited-term license to use, store, host, copy, transmit, modify, create derivative works of, and display Customer Data and Business Contact Information solely as necessary for AvePoint to provide the Solutions and/or Services as the case may be, in accordance with this Agreement. Subject to these limited licenses, AvePoint shall acquire no right, title, or interest from Customer under this Agreement in or to Customer Data or Business Contact Information. Customer grants AvePoint and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Solutions or the Documentation any request, comments, suggestion, recommendation, correction, or other

feedback provided by Customer related to the Solutions (“**Feedback**”). AvePoint may freely use or exploit Feedback in connection with any of its products or services.

2.4. Reserved.

3. OWNERSHIP

Customer agrees that AvePoint or its suppliers retain all right, title, and interest (including all patent, copyright, trademark, trade secret, and other intellectual property rights) in and to the Solutions, all Documentation, deliverables, and any and all related and underlying technology and documentation, and any derivative works, modifications or improvements of any of the foregoing, including as may incorporate Feedback. This Agreement confers no ownership rights to Customer and is not a sale of any rights in the Solutions, the Documentation, or the media on which either is recorded or printed. Customer does not acquire any rights, express or implied, in the Software or the Documentation, other than those rights as a licensee specified in this Agreement. Customer agrees not to disclose, disseminate, or transmit via any medium whatsoever, or make available the Solutions, Software, or any associated trade secrets, to any third party without AvePoint’s prior written consent. AvePoint may generate Usage Data to operate, improve, analyze, and support the Solutions, for benchmarking and reporting and for AvePoint’s other lawful business purposes. Except as expressly set forth in this Agreement, no rights in the Solutions or any AvePoint technology are granted to Customer.

4. ORDERS AND PAYMENT

4.1. Orders. Customer may purchase Solutions by either (a) entering into an Order with AvePoint or (b) entering into an Order with an AvePoint Partner. Each Order with AvePoint shall be signed by both Customer and AvePoint or issued by AvePoint and acknowledged by Customer via the issuance of a purchase order that incorporates by reference the applicable Order and subsequently accepted by AvePoint. All Orders placed through a Partner will be subject to pricing mutually agreed to between Customer and Partner. The use of all Solutions purchased by Customer through either AvePoint or a Partner shall be governed exclusively by this Agreement and, subject to Section 12.15 (Entire Agreement), the applicable Order.

4.2. Invoices.

4.2.1. Purchases from AvePoint. AvePoint shall send, and Customer agrees to receive, electronic invoices in a common format (such as a PDF file). All fees are as set forth in the applicable Order Form and shall be paid by Customer within thirty (30) days from receipt of the invoice, unless otherwise specified in the applicable Order Form. Any late payments shall bear interest from the due date at the interest rate established by the Secretary of the Treasury as provided in [41 U.S.C. 7109](#), which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. If Customer fails to pay the sums provided for in this Agreement (including all addenda hereto) when due, then AvePoint may terminate this Agreement in accordance with Section 10.2 (Termination of this Agreement for Cause).

4.2.2. Purchases Through a Partner. For any Solutions purchased by Customer through a Partner, the pricing and payment terms are established through the Order entered into by and between Customer and such Partner and all payments will be made directly to Partner. AvePoint shall not be liable to Customer or to any third party for any liabilities, claims, or expenses arising from or relating to any suspension or termination of Services in accordance with this Section 4.2.2.

4.3. Disputed Payments. Customer shall have seven (7) business days from the date of an invoice to

dispute a payment. After seven (7) business days from the date of an invoice, all amounts payable to AvePoint shall be deemed undisputed. Disputed amounts shall be clearly defined and listed by Customer with sufficient detail for AvePoint’s review. Once received, AvePoint shall promptly review and answer the notice of dispute. The Parties shall strive in good faith to quickly resolve any disputed amounts. If AvePoint still determines the disputed amount is owed, Customer shall pay the disputed amount or AvePoint may terminate the Agreement for cause in accordance with the Contract Disputes Act and seek damages. Any undisputed amounts on an invoice shall become due and payable, regardless of any disputes about the invoice’s remainder amounts.

4.4. Taxes. AvePoint or its authorized reseller as applicable shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

5. SUPPORT SERVICES

5.1. General. AvePoint Support Services include the following: (1) telephone or electronic support to help Customer correct problems with Solutions; (2) bug fixes and code corrections to correct Solution malfunctions and bring Solutions into substantial conformity with the Documentation; and (3) all upgrades, enhancements, and other changes that AvePoint, at its sole discretion, makes or adds to the Solutions and which AvePoint furnishes, without charge, to all other Customers who receive Support Services. AvePoint shall have the right to verify the existence of any error reported by Customer and AvePoint shall have no obligation to correct any error unless it can be re-created or reproduced by AvePoint with an unaltered version of the Solutions and is not due to incorrect or defective data entry or operator performance by Customer. Customer agrees to provide AvePoint with any information about all programs used by Customer in making its determination that an error exists and shall cooperate in good faith with efforts to resolve any errors. When providing such information, Customer shall not under any circumstances provide personal data to AvePoint for the processing of such data on behalf of Customer, as defined in Article 28.1 GDPR, unless agreed otherwise by way of a separate written agreement between the Parties. AvePoint will then make a prompt and reasonable attempt to provide Customer with a suitable workaround or program change to correct or avoid such error. In the event of on-site services requested by Customer, Customer agrees to reimburse AvePoint for any and all reasonable expenses incurred by AvePoint for purposes of performing such on-site services (including travel expenses in accordance with Federal Travel Regulation (FTR)/Joint Travel Regulations (JTR), as applicable, Customer shall only be liable for such travel expenses as approved by Customer and funded under the applicable ordering document).

5.2. Support Levels. Support Services

provided to Customer during the Support Term are determined by the level of support purchased by Customer (“**Support Level**” or “**Level**”). The Support Level shall be specified in the applicable Order and shall be either Premier, Standard or Basic Level, as further described in the following table:

<u>Support Level</u>	<u>Basic</u>	<u>Standard</u>	<u>Premier</u> (included with all Subscriptions at no additional cost)
Support Channels	Email or Web Support Ticket Only	Email, Web Support Ticket, Phone and Web Conferencing	Email, Web Support Ticket, Phone and Web Conferencing
Support Hours	Business Days, 7:00 am–7:00 pm Local Office Time	Business Days, 7:00 am–7:00 pm Local Office Time	24 hours / day, 7 days / week

5.2.1. Support Level for Subscriptions: All Solutions offered by AvePoint on a Subscription basis include Premier Support Services during the Subscription term stated in the Order.

5.2.2. Support Levels and Payment for Perpetual Licenses: Customers purchasing Licensed Solutions under a perpetual license have the option to purchase Premier, Standard, or Basic Support Services. The fees as provided on the applicable Order or on AvePoint’s invoice to Customer are payable prior to the commencement of any services hereunder. Where an annual payment for multi-year Support Terms has been agreed between the Parties, AvePoint, within its

reasonable discretion, shall invoice Customer approximately forty-five (45) days prior to the beginning of each annual period.

5.3. Support Service Response Times. Support, E-mail, and web support ticket response times shall be based on Issue Severity Level, as defined in the Support Ticket Response Times table below. Such Issue Severity Level shall be assigned by AvePoint at the time of receipt of such e-mail or web support ticket request from Customer per the Issue Description guidelines given in the table below at AvePoint’s sole discretion. AvePoint shall make all commercially reasonable efforts to respond to such support requests within the given Response Time.

<u>Issue Severity Level</u>	<u>Issue Description</u>	<u>E-mail and Web Response Time</u>	<u>Phone Response Time</u>
Low	<ul style="list-style-type: none"> Minor issue which does not impact production environment Documentation error that does not directly impact production Feature or suggestion for enhancement 	48 hours or less	Immediate
Medium	<ul style="list-style-type: none"> An issue affecting production environment at a minor level Very limited direct impact on operations 	24 hours or less	Immediate
High	<ul style="list-style-type: none"> An issue affecting production environment at a major level Production environment is operational, but Solution activities are limited Long-time adverse effects hindering productivity 	4 hours or less	Immediate
Very High	<ul style="list-style-type: none"> Solution activities on production environment are completely inoperable Major restoration or project is at a mission-critical state Severe impact on business operations 	2 hours or less	Immediate

5.4. Support Services for Licensed Solutions.

AvePoint will provide Support Services for Licensed Solutions, including updates and modifications (“Product Releases”), as described under: <https://www.avepoint.com/services/maintenance-support-and-attached-hereto>. For Customers with access to a particular Product Release, AvePoint will provide it in such form and with accompanying instructions sufficient to enable Customer to install it without the assistance of AvePoint. Customer shall be solely responsible for installation of the Product Releases. If requested by Customer, AvePoint will install the Product Release at AvePoint’s daily rates then in effect plus reimbursement for reasonable travel and living expenses incurred by AvePoint and its personnel in providing such installation services in accordance with Federal Travel Regulation (FTR)/Joint Travel Regulations (JTR), as applicable, Customer shall only be liable for such travel expenses as approved by Customer and funded under the applicable ordering document. Customer agrees that any Product Releases provided by AvePoint shall be subject to all of the conditions contained in the Agreement entered into by and between AvePoint and Customer with respect to the Software. Product Releases may update or modify portions of the Software not included as part of Customer’s Licensed Solution. Availability of and access to Product Releases shall not be construed to entitle Customer to new options or features that are sold separately and that are not direct additions to the Licensed Solution to which Customer’s Support Services are associated.

5.5. Exclusions. AvePoint shall not be required to provide any Support Services occasioned by neglect or misuse of the Solutions or equipment using the Solutions, or unauthorized alterations or modifications of the Software. Support Services do not include implementation, configuration, integration, or other custom software development; support for modifications of the Solutions by anyone other than AvePoint or a person acting at AvePoint’s direction; training or “how-to”; assistance with administrative functions; professional services; corrections of immaterial defects; or corrections that will degrade the Solution.

6. WARRANTIES AND DISCLAIMER

6.1. Limited Warranty. For Customer’s benefit only during the Support Term, AvePoint warrants

that the Solutions will substantially conform to the then-current Documentation. AvePoint’s sole liability (and Customer’s sole and exclusive remedy) for any breach of this warranty shall be, at no charge to Customer, for AvePoint to use commercially reasonable efforts to correct the reported non-conformity, or if AvePoint determines such remedy to be impracticable, either party may terminate the applicable Subscription and Customer will receive as its sole remedy a refund of any fees Customer has pre-paid for use of the applicable Solutions for the terminated portion of the applicable Subscription Term. The limited warranty in this Section 6.1 shall not apply: (i) unless Customer makes a claim within thirty (30) days of the date on which Customer first noticed the non-conformity, (ii) if the error was caused by misuse, unauthorized modifications or third-party hardware, software or services, or (iii) to Beta Releases or any use of the Solutions provided on a no-charge or evaluation basis.

6.2. Warranty Disclaimer. EXCEPT FOR THE LIMITED WARRANTIES STATED ABOVE, THE SOLUTIONS AND ALL RELATED SERVICES ARE PROVIDED “AS IS” AND CUSTOMER’S USE OF THEM IS AT ITS OWN RISK. AVEPOINT DOES NOT MAKE, AND HEREBY SPECIFICALLY DISCLAIMS, AND CUSTOMER RELEASES AND WAIVES, ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE OR FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE OR TRADE PRACTICE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. AVEPOINT DOES NOT WARRANT THAT CUSTOMER’S USE OF THE SOLUTIONS WILL BE UNINTERRUPTED OR ERROR-FREE, NOR DOES AVEPOINT WARRANT THAT IT WILL REVIEW CUSTOMER DATA FOR ACCURACY OR THAT IT WILL PRESERVE OR MAINTAIN CUSTOMER DATA WITHOUT LOSS. AVEPOINT SHALL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES OR OTHER PROBLEMS INHERENT IN USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF AVEPOINT. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, AVEPOINT DOES NOT WARRANT THAT THE SOLUTIONS WILL MEET CUSTOMER’S REQUIREMENTS, WILL OPERATE IN ANY COMBINATION THAT MAY BE SELECTED FOR USE BY CUSTOMER OR IN COMBINATION WITH OTHER THIRD-PARTY SOFTWARE BEYOND THE THIRD- PARTY SOFTWARE EXPRESSLY APPROVED AS

COMPLIANT IN THE DOCUMENTATION. EXCEPT AS TO COMPATIBILITY OF THE LICENSED SOFTWARE AS DESCRIBED IN AVEPOINT'S DOCUMENTATION, AVEPOINT MAKES NO WARRANTIES TO CUSTOMER WITH RESPECT TO CUSTOMER'S COMPUTER EQUIPMENT OR SYSTEM SOFTWARE OR ITS CAPACITY. FURTHERMORE, AVEPOINT DOES NOT WARRANT THAT ANY SOFTWARE ERRORS, DEFECTS, OR INEFFICIENCIES WILL BE CORRECTED, NOR DOES AVEPOINT ASSUME ANY LIABILITY FOR FAILURE TO CORRECT ANY SUCH ERROR, DEFECT OR INEFFICIENCY. AVEPOINT MAKES NO WARRANTY, AND CUSTOMER ASSUMES THE ENTIRE RISK, AS TO THE INTEGRITY OF ANY DATA AND THE RESULTS, CAPABILITIES, SUITABILITY, USE, NON-USE OR PERFORMANCE OF THE SOLUTIONS. IN NO EVENT SHALL AVEPOINT BE LIABLE TO CUSTOMER FOR ANY DAMAGES RESULTING FROM OR RELATED TO THE USE OF THE SOLUTIONS. CUSTOMER MAY HAVE OTHER STATUTORY RIGHTS, BUT THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE SHORTEST PERIOD PERMITTED BY LAW.

7. REMEDIES AND DAMAGES LIMITATION

7.1. Consequential Damages Waiver.

NEITHER PARTY SHALL HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOSS OF USE, LOST DATA, LOST PROFITS, FAILURE OF SECURITY MECHANISMS, INTERRUPTION OF BUSINESS, LOSS CAUSED BY THE INTERRUPTION, TERMINATION OR DELAYED OPERATION OF THE INTERNET, THIRD-PARTY TELECOMMUNICATION SERVICES OR THIRD-PARTY SECURITY FEATURES OR SYSTEMS, EXCEPT AS REQUIRED BY LAW. EXCEPT FOR CUSTOMER'S BREACH OF SECTION 1.4 (USE RESTRICTIONS) OR EITHER PARTY'S UNLAWFUL OR WILLFUL MISCONDUCT OR GROSS NEGLIGENCE, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF INFORMED OF THE POSSIBILITY IN ADVANCE, SUFFERED BY ANY PARTY OR ANY PARTY CLAIMING ON BEHALF OF OR THROUGH THE OTHER PARTY, OR ANY OTHER THIRD PARTY RESULTING FROM OR ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PERFORMANCE OR BREACH THEREOF. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S GROSS

NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

7.2. Liability Cap. EXCEPT FOR EXCLUDED CLAIMS, EACH PARTY'S ENTIRE CUMULATIVE LIABILITY TO THE OTHER ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT, IN THE CASE OF AVEPOINT, EXCEED THE AMOUNT ACTUALLY PAID BY CUSTOMER TO AVEPOINT UNDER THIS AGREEMENT DURING THE TWENTY-FOUR

(24) MONTHS PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY OR, IN THE CASE OF CUSTOMER, EXCEED THE AMOUNT PAYABLE TO AVEPOINT IN ACCORDANCE WITH THE ORDER. FOR THE AVOIDANCE OF DOUBT, THE PRECEDING LIMITATION OF LIABILITY SHALL NOT AFFECT CUSTOMER'S OBLIGATION TO EFFECT PAYMENT AS PER SECTION 4 (ORDERS AND PAYMENT), WHICH SHALL REMAIN IN EFFECT REGARDLESS OF AND ON TOP OF THE LIMITATION OF LIABILITY.

7.3. Excluded Claims. "Excluded Claims"

means (a) any claim arising from Customer's breach of Section 1.4 (Use Restrictions), 2.3 (Rights in Customer Data); (b) any amounts payable to third parties pursuant to Customer's indemnification obligations under Section 2.4 (Indemnification by Customer) or AvePoint's indemnification obligations under Section 8 (Indemnification); (c) Customer's breach of Section 3 (Ownership); or (d) unlawful or willful misconduct or gross negligence.

7.4. Nature of Claims and Failure of Essential Purpose.

The Parties agree that the waivers and limitations specified in this Section 7 apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise, and will survive and apply even if any limited remedy specified in this Agreement is found to have failed of its essential purpose.

8. INDEMNITY

AvePoint shall have the right to defend Customer from and against any claim by a third party alleging that the Solutions when used as authorized under this Agreement infringes a patent or any copyright or trademark and shall indemnify and hold harmless Customer from and against any damages and costs awarded against Customer or agreed in settlement by AvePoint (including reasonable attorneys' fees)

resulting from such claim, provided that AvePoint has received from Customer: (i) prompt written notice of such claim (but in any event notice in sufficient time for AvePoint to respond without prejudice); (ii) the = right to control and direct the investigation, defense and settlement (if applicable) of such claim; and (iii) all reasonably necessary cooperation of Customer (at AvePoint's expense for reasonable out-of-pocket costs). Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. If Customer's use of the Solutions is (or in AvePoint's opinion is likely to be) enjoined, if required by settlement or if AvePoint determines such actions are reasonably necessary to avoid material liability, AvePoint may, in its sole discretion: (a) substitute substantially functionally similar products or services; (b) procure for Customer the right to continue using the Solutions; or if (a) and (b) are not commercially reasonable, (c) terminate the Agreement and refund to Customer the fees paid by Customer for the portion of the Subscription Term that was paid by Customer but not rendered by AvePoint. The foregoing indemnification obligation of AvePoint shall not apply: (1) if the Solutions are modified by any party other than AvePoint, but solely to the extent the alleged infringement is caused by such modification; (2) if the Solutions are combined with products or processes not provided by AvePoint, but solely to the extent the alleged infringement is caused by such combination; (3) to any unauthorized use of the Solutions; (4) to any action arising as a result of Customer Data or any third-party deliverables or components contained within the Solutions; or (5) if Customer settles or makes any admissions with respect to a claim without AvePoint's prior written consent. THIS SECTION 8 SETS FORTH AVEPOINT'S AND ITS SUPPLIERS' SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

9. CONFIDENTIAL INFORMATION

Each party (as "**Receiving Party**") agrees that all code, inventions, know-how, privacy and/or security reports, business, technical and financial information and trade secrets obtained from 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 should be reasonably known by the Receiving Party to be confidential or proprietary due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any AvePoint technology, performance information relating to the Services, and the terms and conditions of this Agreement shall be deemed Confidential Information of AvePoint without any marking or further designation. Except as expressly authorized herein, the Receiving Party shall (1) hold in confidence and not disclose any Confidential Information to third parties except to its own or its Affiliates' directors, officers, employees, auditors, agents, consultants or other representatives, provided that these persons have a clear need to know such Confidential Information in connection with the Purpose and are bound by an obligation of confidentiality no less restrictive than set forth in this Agreement, and provided that the Receiving Party remains responsible for compliance by any such representative with the terms of this Section; and (2) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement. The Receiving Party's confidentiality obligations shall not apply to information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the Receiving Party who had no access to such information. The Receiving Party may make disclosures to the extent required by law or court order, provided the Receiving Party – to the extent legally permitted – notifies the Disclosing Party in advance and cooperates in any effort to obtain confidential treatment. AvePoint recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor, but shall, if possible, be given an opportunity to support its classification of the information as "confidential."

10. TERM AND TERMINATION

10.1. Term. This Agreement shall remain in full force and effect from the Effective Date until terminated pursuant to Section 10.2 (Termination of this Agreement for Cause), or as otherwise agreed by the Parties in writing when Customer's Subscriptions have expired or been terminated in accordance with this Agreement.

10.1. Termination of this Agreement for Cause. In accordance with the Contract Disputes Act, AvePoint shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Notwithstanding the foregoing, a Party shall not be permitted to terminate this Agreement due to that Party's own material breach of this Agreement.

10.2. Effect of Termination. Immediately upon termination, cancellation, or expiration of this Agreement for any reason, all rights and Licenses granted to Customer shall cease and terminate, and Customer shall have no right thereafter to use, and shall cease the use of, the Solutions. Where applicable, Customer shall uninstall any Licensed Solutions from its systems and shall, at AvePoint's sole discretion, either destroy or return the Licensed Solutions (including all copies thereof) to AvePoint. Except as set out in Section 10.3 (Data Retention and Migration of Generated Data) below, Customer acknowledges that following termination, cancellation, or expiration of this Agreement or any Subscription, it shall have no further access to any Customer Data in the SaaS Solutions, and, except as provided elsewhere in this Agreement, that AvePoint may delete any such data as may have been stored by AvePoint at any time. Except where an exclusive remedy is specified, the exercise of either party of any remedy under this Agreement, including termination, will be without prejudice to other remedies it may have under this Agreement, by law or otherwise. If Customer terminates pursuant to Section 10.2 for cause, then Customer shall be entitled to a refund of pre-paid fees for Maintenance or subscription-based Solutions for the remaining months in the then-current Support Term or Subscription Term (as applicable).

10.3. Data Retention and Migration. Upon cancellation, termination or expiration of a Subscription or termination of this Agreement,

Customer Data in the SaaS Solutions will be preserved for thirty (30) days (the "**Retention Period**") and, upon request, made available to Customer within a commercially reasonable timeframe. After the Retention Period, such Customer Data will be permanently deleted from AvePoint's Server and unrecoverable by Customer. After the Retention Period, AvePoint makes no representations or warranties as to the preservation or integrity of Customer Data. Customer hereby agrees that AvePoint shall have no obligation to retain Customer Data after the Retention Period, unless otherwise prohibited by law. If Customer renews its Subscription to the SaaS Solutions prior to the end of the Retention Period, Customer Data shall remain available to Customer. Before the Retention Period ends, Customer may request AvePoint to provide certain data migration and/or export services: (1) Generated Data Export Services- Providing a copy of the Customer's Generated Data for export to another Cloud Storage Provider or on-premises location of Customer's choosing; or (2) Data Migration Services- Migration services to assist in the transitioning to or from Customer-provided storage to or from alternative storage of Customer's choosing, or migration of data between Customer's online services tenant and another online services tenant, whether within the same region or across regions. In either instance, AvePoint shall assess whether and to what extent such export/migration is reasonably possible. If AvePoint elects to provide such services, it will do so at its then current rates, unless otherwise agreed in writing between AvePoint and Customer.

10.4. Surviving Provisions. The following Sections shall survive any expiration, cancellation, or termination of this Agreement: 1.4 (Use Restrictions), 2.3 (Rights in Customer Data), 2.4 (Indemnification by Customer), 3 (Ownership), 4 (Fees), 6.1 (Warranty Disclaimer), 7 (Limitation of Remedies and Damages), 8 (Indemnification), 9 (Confidential Information), 10 (Term and Termination), and 12 (General Terms).

10.5. Termination or Expiration of Subscriptions and Support Services. Expiration or termination of any Subscription or of Support Services for Perpetual Licenses may occur without termination of the Agreement. Unless terminated in accordance with the Agreement, a Subscription or Support Service shall continue in force for the period provided for in the Order (the "**Initial Term**"). The Subscription shall thereafter may be renewed for

renewal terms of one (1) year (“**Renewal Term**”) by executing a written order for the Renewal Term at then current GSA Schedule Pricelist rates.

11. CO-MARKETING. Customer agrees to the use of Customer’s name on AvePoint’s web site and promotional materials, in press releases, product brochures, sales presentations, financial reports, webinars, and in other public statements or releases to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71. Customer agrees that AvePoint may disclose Customer as a customer of AvePoint.

12. GENERAL TERMS

12.1. Definitions.

“**Affiliate**” means, with respect to any person, any other person that controls or is controlled by or under common control with such Person; provided, that a person shall be deemed to be an Affiliate only so long as such control exists. For the purposes of this definition, “**person**” means any individual, corporation, partnership, joint venture, joint stock company, trust, estate, association, limited liability company, or other entity the existence of which is recognized by any legal or regulatory authority; and “**control**,” when used with respect to any Person, means direct or indirect ownership of at least fifty percent (50%) of the voting stock, shares, or other equity interest in the controlled Person and possession of the power to direct or cause the direction of the management and policies of the controlled Person.

“**Authorized User**” or “**User**” means: (i) a direct user of the Solutions, including but not limited to Customer’s and Customer’s Affiliates’ employees; or (ii) Customer’s and Customer’s Affiliates’ consultants who have agreed to use the Solutions only for the benefit of Customer and Customer’s Affiliates and subject to the terms and conditions and restrictions of this Agreement. For the avoidance of doubt, Customer is responsible for ensuring such compliance of its consultants.

“**Business Contact Information**” means incidental business contact information that Customer provides to AvePoint in the ordinary course of business, which AvePoint in turn retains within various internal systems and departmental records, including but not limited to its customer relationship management system, Legal and Accounting

departments.

“**Cloud Storage Provider**” means the third party that provides AvePoint with cloud storage capacities to store Customer Data and provide the Solutions. Depending on the AvePoint Solution for which Customer purchased an access right, certain Customer Data may be stored on supported cloud storage capacities of a different Cloud Storage Provider that is contracted by Customer.

“**Customer Data**” means data that is: a) provided to AvePoint by, or on behalf of, Customer (including all text, sound, video, or image files, and software) for use with the Solutions (“**Customer Provided Data**”); b) referring to Customer specific configurations that are necessary for the operation of the Solutions (“**Configuration Data**”); or c) generated from Customer Provided Data by features of the Solutions and hosted on the storage of the Cloud Storage Provider, e.g. generated backups of Customer Provided Data or log files generated by the Solutions (“**Generated Data**”).

“**Defect**” means a problem causing the Solution to not materially or substantially conform to the Documentation.

“**Documentation**” means the end user documentation delivered with or related to the Solutions (including but not limited to user guides, manuals, release notes or online portals and wiki pages) as may be modified from time to time including, but not limited to, user guides at <https://www.avepoint.com/resources/user-guides>.

“**Downtime**” means the total accumulated time during which the relevant Solutions are without external connectivity, meaning without bi-directional network traffic over supported protocol.

“**DPIS Policy**” is AvePoint’s Data Protection and Information Security Policy as periodically amended: <https://www.avepoint.com/license/dataprotection.html>.

“**Internal Use**” means use of the Solutions by employees of Customer in Customer’s internal operations but does not include access of the Solutions by, or use of the Solutions in the provisions of services to, Customer’s clients or customers. Internal Use also includes use of the Solutions by contractors of Customer, including contractors providing outsourcing or hosting services, as long as Customer assumes full

responsibility for the compliance with this Agreement in such use. Use of the Solutions (or any part thereof) for the benefit of others, whether by means of a software as a service offering, application service provider, outsourcing or other means of providing service to any third party shall not be considered Internal Use.

“Licensed Solution” means the Software for which Customer has purchased a License as identified in an Order, including updates or upgrades to it that AvePoint may at its discretion deliver to Customer.

“Local Office Time” means the given time at the nearest appropriate AvePoint office or Call Center designated to provide Support Services to Customer at AvePoint’s discretion.

“Order” or **“Order Form”** means a valid order by Customer, which can be a) an AvePoint sales quote that has been signed by Customer; b) a Customer purchase order that has been accepted by AvePoint; or c) where Customer purchases through a Partner, the relevant purchase document that has been accepted. For the avoidance of doubt, any (pre-printed) terms of Customer or references thereto on Customer purchase orders or like order documents shall not be applicable.

“Partner” means a reseller or distributor of AvePoint with which AvePoint is party to an agreement memorializing that relationship accordingly.

“Perpetual License” means a perpetual license to the Software that is identified in the pertaining applicable Order and is subject to the limitations set forth in Sections 1.2.1.2 (Perpetual Licenses) and 1.4 (Use Restrictions).

“Personal Data” has the meaning given to it in the EU Regulation 2016/679 (**“General Data Protection Regulation”** or **“GDPR”**).

“SaaS Solution” means the specific AvePoint proprietary hosted service(s) specified on an Order form, including any related AvePoint dashboards, APIs, and AvePoint Software.

“Service Credit” means the percentage of the total fees paid for specific SaaS Solutions that are applied to the month (i.e., 1/12 of the annual fees owed by Customer to AvePoint for the specific SaaS Solutions) in which a Service Credit is owed. If Customer purchased SaaS Solutions as part of a suite or other

single offer, the monthly fees and Service Credit for each SaaS Solution will be pro-rated.

“SharePoint Server” means a configured and installed server (whether physical or virtual) on which the Microsoft SharePoint application is run.

“Software” means the object code (machine readable) version of any computer programs offered by AvePoint and any ancillary data files, modules, libraries, tutorial or demonstration programs or other components and copies of any of the foregoing or portions thereof.

“Solutions” means the SaaS Solutions and/or Licensed Solutions for which Customer is purchasing an access right or a License (as applicable) pursuant to this Agreement and the corresponding Order.

“Subscription” means the metric according to which SaaS Solutions or Term Licenses are purchased on a non-perpetual basis, as described in the Order.

“Term” means the period specified in the applicable Order during which Customer will be granted a) access to the SaaS Solutions; b) a Term License, as applicable; or c) Support Services. For SaaS Solutions and Term Licenses, the Support Term shall be equal to the Subscription Term.

“Usage Data” means AvePoint’s technical logs, data and learnings about Customer’s use of the Services (e.g., frequency of logins). For clarity, Usage Data does not include Customer Data.

12.2. Binding Effect. This Agreement and all of the provisions hereof shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors and permitted assigns.

12.3. Amendment. This Agreement may be amended only by a writing duly executed by the authorized representatives of the Parties hereto which makes specific reference to this Agreement.

12.4. Notices. All notices, requests, demands, consents, authorizations, claims, and other communications (each a “Notice”) hereunder must be in writing by an authorized representative of the sender and shall be deemed to have been duly given: (i) when hand-delivered to the addressee; (ii) when transmitted by confirmed e-mail with a duly

signed scan of the Notice attached; (iii) one (1) business day after being given to an overnight courier with a reliable system for tracking delivery; or (iv) three (3) business days after the day of mailing, when mailed by registered or certified mail, return receipt requested, postage prepaid. Notices to AvePoint shall be sent, Attn: General Counsel, 901 E. Byrd Street, Suite 900, Richmond, VA 23219; or, if sent by confirmed e-mail, to legal@avepoint.com. Unless otherwise specified by Customer in writing, Notices to Customer shall be sent to Customer's e-mail address provided in the Order or, if no such e-mail address has been provided, to the registered agent of Customer in the jurisdiction in which Customer is organized or incorporated. Any Party may change the address to which Notices are to be delivered by giving the other Party Notice in the manner herein set forth.

12.5. Intentionally Omitted.

12.6. Assignment. Customer may not, directly or indirectly, sell, assign, sublicense, lease, rent, distribute, or otherwise transfer the Agreement or any rights or obligations therein to any other person or entity without AvePoint's written consent.

12.7. Waiver. No Party shall be deemed to have waived any of its rights, powers or remedies under this Agreement unless such waiver is expressly set forth in a writing signed by the waiving Party. No written waiver of any provision of this Agreement shall be deemed to be, or shall constitute, (i) a waiver of any other provision of this Agreement, whether or not similar, or (ii) a continuing or subsequent waiver of the same or another provision of this Agreement. The failure of either Party to enforce at any time any of the provisions of this Agreement, or the failure to require at any time performance by the other Party of any of the provisions of this Agreement, will in no way be construed to be a present or future waiver of any such provisions, or in any way affect the validity of either Party to enforce each and every such provision thereafter.

12.8. Force Majeure. Excusable delays shall be governed by GSA Schedule Contract Clause 552.212-4(f)

12.9. Captions. The captions and headings of Sections and subsections contained in this Agreement are provided for convenience of reference only and shall not be considered a part hereof for purposes of interpreting this Agreement, and, therefore, such captions and headings do not define, modify, limit, describe or affect in any way the meaning or intent of this Agreement or any of its terms or provisions.

12.10. Severability. If any Section or other provision of this Agreement, or the application of such Section or provision, is held invalid, then the remainder of this Agreement, and the application of such Section or provision to persons or circumstances other than those with respect to which it is held invalid, shall not in any way be affected or impaired thereby. If any provision of this Agreement becomes or is declared by a court of competent jurisdiction or panel of arbitrators to be illegal, unenforceable or void, this Agreement shall continue in full force and effect without said provision. The Parties agree to negotiate in good faith a substitute valid and enforceable provision that most nearly effects the Parties' intent and to be bound by the mutually agreed substitute provision.

12.11. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original but all of which together will constitute one and the same instrument.

12.12. Segmentation. Any of Customer's purchases under this Agreement are separate Orders and are separate from any other offer that Customer may receive or may have received from AvePoint. Customer understands that it may purchase any AvePoint Solutions independently of any other purchase from AvePoint. Customer's obligation to pay for any purchase is not contingent on the performance and/or delivery of any other purchase from AvePoint.

12.13. Remedies. All remedies shall be cumulative and not alternative and in addition to all other rights and remedies available in law and in equity.

12.14. Intentionally Omitted.

12.15. Entire Agreement. This Agreement, including any referenced or attached addenda,

exhibits, and/or appendices (which shall be deemed incorporated by this reference), is the complete and exclusive statement of the mutual understanding of the Parties. Notwithstanding the foregoing, to the extent that there exists a Prior Negotiated Agreement, the provisions of that Prior Negotiated Agreement shall control unless expressly provided otherwise in such other agreements. In the event that there is no such Prior Negotiated Agreement, then the provision of the Solutions by AvePoint, and Customer's use thereof, shall be governed by this Agreement. Subject to anything to the contrary contained in this Agreement or any Prior Negotiated Agreement, this Agreement between the Parties supersedes and cancels as null and void any and all prior and contemporaneous negotiations, discussions, proposals, agreements, representations or communications, oral or written, of the Parties with respect to the subject matter. Notwithstanding the foregoing, an Order form submitted by Customer and accepted by AvePoint may set forth only the type, description and quantity of Services and provide for a longer Support Term or for a longer Subscription Term, and such terms shall be deemed binding. No other purchase order terms or conditions of Customer shall be deemed to supersede, replace, or modify this Agreement. There are no representations, agreements, arrangements, or understandings, oral or written, between the Parties relating to the subject matter of the Agreement which are not fully expressed. In this Agreement, headings are for convenience only and "including", "e.g.", and similar terms will be construed without limitation.

12.16. Subpoenas. Nothing in this Agreement prevents AvePoint from disclosing Customer Data to the extent required by law, subpoenas, or court orders. AvePoint shall use commercially reasonable efforts to notify Customer where permitted to do so.

12.17. Independent Contractors. Customer and AvePoint are independent contractors. There is no relationship of partnership, joint venture, employment, franchise, or agency between the parties. Neither Party can bind the other or incur obligations on the other Party's behalf without the other Party's prior written consent.

12.18. Export Control. Customer shall comply with all export and import laws and regulations of the United States and other applicable jurisdictions governing use, export, reexport, and transfer of

products, technology, and services and will obtain all necessary or required authorizations, permits, and licenses. Without limiting the foregoing, Customer represents and warrants that it is not, and it will not permit access to the Solutions by any user who is (i) designated on the Specially Designated Nationals and Blocked Persons List, the Consolidated Sanctions List, or any other list administered by Office of Foreign Assets Control of the U.S. Treasury Department, (ii) designated on the Denied Persons List, the Unverified List, the Entity List, or any other list administered by the U.S. Commerce Department, (iii) designated on any list of targeted persons issued under the economic, financial, trade or investment sanctions of the United Nations, the European Union, or any other country, (iv) a government of a Sanctioned Territory, the government of Venezuela, or an Iranian bank, (v) located within, operating from, or national of a Sanctioned Territory, or (vi) owned or controlled by, or acting on behalf of, any of the foregoing. For the purposes of this section, "**Sanctioned Territory**" means any country or other territory subject to a general export, import, financial or investment embargo or restriction under U.S. or other applicable law, which as of March 2022, includes Cuba, Iran, North Korea, Syria, Russia, Belarus, and the Crimea, Donetsk People's Republic, and Luhansk People's Republic regions of Ukraine. Customer shall not submit to the Solution any information that is controlled under the U.S. International Traffic in Arms Regulations. Customer represents and warrants that it will not use the Solutions for any purposes prohibited by U.S. law, including, without limitation, the development, design, manufacture, or production of missiles or nuclear, chemical, or biological weapons. Customer shall immediately notify AvePoint if it has any information or suspicion that there may be a violation of this Section. Customer also represents and warrants that it is aware of, understands, and agrees to comply with, and to avoid any activity that may cause it or AvePoint to violate, applicable anti-bribery and anti-corruption laws including, but not limited to, the U.S. Foreign Corrupt Practices Act of 1977 (15 U.S.C. §§ 78dd-1, et seq.) as amended and the UK Bribery Act 2010 (as applicable) (collectively, "Anti-Corruption Laws"). If Customer takes any action that could constitute a violation of this Section or any Anti-Corruption Laws, AvePoint may immediately terminate this Agreement.

12.19. Government End-Users. If the user or licensee of the Solutions is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Solutions, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by this Agreement in accordance with Federal Acquisition Regulation 12.212. The Solutions were developed fully at private expense. All other use is prohibited.

12.20. Counterparts. This Agreement may be executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.

Appendix A

AvePoint's Privacy Policy

<http://www.avepoint.com/company/privacy-policy>

1. Information We Collect

1.1 Summary

AvePoint collects many kinds of information in order to operate effectively and provide you the best products, services and experiences we can. We collect information when you register, sign in and use our sites and services. We also may get information from other companies. We collect this information in a variety of ways, including from web forms, technologies like cookies, web logging and software on your computer or other device.

AvePoint products use and transfer data only using recommended methodologies and APIs approved by Microsoft, Google, Salesforce, or other platform technology providers. Our applications' use of APIs adheres to the respective user data policies of such platform technology providers, as applicable. For example, our use of Google APIs adheres to the [Google API Services User Data Policy](#) (including Google's "Limited Use" requirements thereunder).

We use information submitted through our websites or collected through email or hard copy surveys to analyze the characteristics of our customers and improve our services. Occasionally, we will provide anonymized aggregated statistics about our customers in reports made available to our customers, to third parties, or to the public. These reports will not identify individual AvePoint customers.

If you request information about AvePoint products and services, we will collect your name, email address, phone number, and additional company information. We use this information to contact you about your request, and to follow up with you about the products and services in which you have expressed an interest. We will also send information to you regarding upcoming AvePoint events, webinars, and relevant privacy related news and alerts. You may unsubscribe from these communications at any time by clicking on the unsubscribe link provided in the email.

AvePoint receives and processes information (in paper and electronic form) in accordance with its clients' instructions for the purpose of providing services to its customers. At AvePoint, we recognize the importance of privacy to our customers and we strive to safeguard any personal information we receive and may need to use in support of our customers.

We respect each individual's right to personal privacy. We will collect and use information we receive directly from you only in the ways disclosed in this Privacy Policy. This policy does not apply to practices that AvePoint does not own or control, or to individuals that AvePoint does not employ or manage. For transfers of personal data between our entities in the European Union and other AvePoint entities, AvePoint has entered into Standard Contractual Clauses ("SCCs") with all of its affiliated companies in order to ensure an adequate level of protection of such personal data. In addition to the protection under the SCCs, AvePoint (including its controlled U.S. subsidiaries) adheres to the set of data protection principles developed by the United States Department of Commerce (DOC), in collaboration with the European Commission, which produced the U.S.-European Union Privacy Shield Framework Documents. AvePoint further adheres to the Swiss-U.S. Privacy Shield Framework. The privacy principles in this policy are based on the SCCs and these Privacy Shield principles ("Privacy Shield Principles") and are further articulated in the AvePoint Privacy Shield Policy ("Privacy Shield Policy") available at <https://www.avepoint.com/company/privacy-shield-policy/> that sets out the privacy principles to which AvePoint adheres. AvePoint has furthermore certified to the DOC that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Policy (including AvePoint's obligations stemming from its compliance with the SCCs) and the Privacy Shield Principles, the terms in this Privacy Policy shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>.

This published Privacy Policy and the Privacy Shield Policy are accurate, comprehensive, prominently displayed, completely implemented, accessible and conform to the SCCs and the Privacy Shield Principles. In addition, we provide appropriate employee training (and discipline) and have internal procedures for periodically conducting objective reviews of our compliance with the SCCs and the Privacy Shield Principles.

1.2 Full text

AvePoint collects many kinds of information in order to operate effectively and provide you the best

products, services and experiences we can. Some of this information you provide directly to us. Some of it we get by observing how you interact with our products and services. Some of it is available from other sources that we may combine with the data we collect directly. Regardless of the source, we believe it's important to treat that information with care and to help you maintain your privacy.

What we collect:

- Registration

When you sign up to use our sites or services you may be required to provide information about yourself, such as your name, birthdate, organization name, e- mail and postal address and postal code.

- Signing in

To access some AvePoint services, you will need to sign in with a user name and password, which we refer to as your user account.

- Using our sites and services

We collect information that tells us how you interact with our services, including the browser you're using, your IP address, location, cookies or other unique IDs, the pages you visit and features you use.

- Data from other sources

We may get additional information about you, such as demographic data we purchase from other companies.

How we collect:

We use a number of methods and technologies to gather information about how you use our sites and services, such as:

- Web forms, such as when you type information into a registration form or type a search query into a search box.

- Technologies like cookies and web beacons (Please visit Section 2 of this Privacy Policy page to learn more about these technologies).

- Web logging, which enables us to collect the standard information your browser sends to every web site you visit - such as your IP address, browser type and language, and the site you came from - as well as the pages you visit and the links you click while using our sites and services.

- Software installed on your computer or other device, which may send back information needed to operate, update or improve that software.

Customer Data:

AvePoint receives and processes information (in paper and electronic form) in accordance with its clients' instructions for the purpose of providing services to its customers. At AvePoint, we recognize the importance of privacy to our customers and we strive to safeguard any personal information we receive and may need to use in support of our customers.

AvePoint Customer Information

Customer Information is information we collect from you when you purchase and contract with us to provide services or technology solutions. We will ask you to provide the following information:

- Email address;
- Phone number;
- Information regarding your role within your company;
- Company information, including company name, address, billing information (e.g., P.O. number, bank wire information, credit card number), and company size; and
- Contact information for other relevant points of contact within your company as needed for AvePoint to provide its services.

If you purchased one of AvePoint's technical solutions you may have the option to add additional users to your account. We will ask for the name and email address of the additional users you want to add. This information is used by AvePoint to provide the requested service.

In the course of using AvePoint's technical solutions or services, you may provide business information related to your company. Business information may include copies of your company's policies and process documents, responses to assessment questionnaires and evidence to support those responses. This information is stored on AvePoint's systems, and is used to provide contracted services in accordance with the applicable terms and conditions of agreements between AvePoint and your company.

2. Cookies & Similar Technologies

2.1 Summary

Most AvePoint web sites use "cookies," small pieces of data that can be read by a web server in the same domain that put the cookie on your hard drive. We may use cookies to help us retrieve your preferences and settings; help with sign-in; to combat fraud; and analyze site operations.

We also use web beacons to help deliver cookies and compile analytics. These may include third-party web beacons, which are prohibited from collecting your personal information.

You have a variety of tools to control cookies and similar technologies, including:

- Browser controls to block and delete cookies; and
- Controls from some analytics providers to opt out of data collection in web beacons.

2.2 Full text

2.2.1 Our Use of Cookies

Most AvePoint web sites use "cookies," which are small pieces of data sent to your browser by a web server. Upon subsequent requests, your browser will send the cookie data to the same web server, or other web servers in the same domain, when accessing the web site. Cookies contain data that can be read by a web server in the domain that issued the cookie to you. That data often consists of a string of numbers and letters that uniquely identifies your computer, but may contain other information as well. Here is an example of a unique ID number stored in a cookie that AvePoint might place on your device when you visit one of our web sites: 0aj17be34l7srju0qcdnftigt0

We may use cookies for:

- Sign-in and Authentication

When you sign in to a site or service using your account on an AvePoint web site, we store a unique ID number, and the time you signed in, in an encrypted cookie on your hard disk. This cookie allows you to move from page to page at the site without having to sign in again on each page. When you sign out, these cookies are deleted from your computer. This is commonly referred to as a "session cookie".

We also use cookies to improve the sign-in experience. For example, your user name may be stored in a cookie that will remain on your computer after you sign out. This cookie allows your user name to be pre-populated, so that you will only need to type your password the next time you sign in. If you are using a public computer or do not want this information to be stored, you can select the appropriate radio button on the sign-in page, and this cookie will not be used.

- Site Analytics

We may use cookies to count the number of unique visitors to a web page or service or to develop other aggregate statistics about the operations of our sites and services. These analytics help us operate and improve the performance of these sites and services.

In addition to the cookies AvePoint may set when you visit our web sites, third parties may also set certain cookies on your device when you visit AvePoint sites. In some cases, that is because we have hired the third party to provide certain services on our behalf, such as site analytics. In other cases, it is because our web pages contain content or ads from third parties, such as videos, news content or ads delivered by other ad networks. Because your browser connects to those third parties' web servers to retrieve that content, those third parties are able to set or read their own cookies on your device and may collect information about your online activities across websites or online services.

2.2.2 How to Control Cookies

- Browser Controls to Block Cookies.

Most web browsers automatically accept cookies, but you can usually modify your browser setting to block cookies. Instructions for blocking cookies in different browsers are usually available at each browser's privacy statement or in their help files or settings pages.

Please be aware that if you choose to block cookies, you may not be able to sign in or use other interactive features of AvePoint sites and services that depend on cookies.

- Browser Controls to Delete Cookies

If you accept cookies, you can delete them later. Instructions for deleting cookies in different browsers are usually available at each browser's privacy statement or in their help files or settings pages.

Please be aware that if you choose to delete cookies, any settings and preferences controlled by those cookies will be deleted and may need to be recreated.

- Browser Controls for "Do Not Track" and Tracking Protection

Some newer browsers have incorporated "Do Not Track" features. Most of these features, when turned on, send a signal or preference to the web sites you visit indicating that you do not wish to be tracked. Those sites (or the third party content on those sites) may continue to engage in activities you might view as tracking even though you have expressed this preference, depending on the sites' privacy practices. Because there is not yet a common understanding of how to interpret the DNT signal, AvePoint does not currently respond to the browser DNT signals on its own websites or online services, or on third-party websites or online services where AvePoint provides content or is otherwise able to collect information.

2.2.3 Our Use of Web Beacons

AvePoint web pages may contain electronic images known as web beacons - sometimes called singlepixel gifs - that may be used to help deliver cookies on our sites, let us count users who have visited those pages and deliver co-branded services. We may include web beacons in our promotional e-mail messages or newsletters to determine whether messages have been opened and acted upon.

Finally, AvePoint sites may contain web beacons from third parties to help us compile aggregated statistics regarding the effectiveness of our promotional campaigns or other web site operations. These web beacons may allow the third parties to set or read a cookie on your computer. These companies may collect information about your online activities across websites or online servers, however, we prohibit third parties from using web beacons on our sites to collect or access your personal information. You may be able to opt out from data collection or use by these third-party analytics companies by opting out on their respective web sites.

2.2.4 Other Similar Technologies

In addition to standard cookies and web beacons, web sites can use other technologies to store and read data files on your computer. This may be done to maintain your preferences or to improve speed and performance by storing certain files locally. But, like standard cookies, it can also be used to store a unique identifier for your computer, which can then be used to track behavior. These technologies include Local Shared Objects (or "Flash cookies"), HTML5 Local Storage and Silverlight Application Storage.

- Local Shared Objects or "Flash cookies"

Web sites that use Adobe Flash technologies may use Local Shared Objects or "Flash cookies" to store data on your computer. Note that the ability to clear Flash cookies may or may not be controlled by your browser setting for standard cookies as that may vary by browser. To manage or block Flash cookies, go to the appropriate settings page, currently to be found

at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html.

- Silverlight Application Storage

Web sites or applications that use Microsoft Silverlight technology also have the ability to store data by using Silverlight Application Storage. To learn how to manage or block such storage, visit the Silverlight Privacy Statement.

3. How We Use Your Personal Information

3.1 Summary

AvePoint uses the information we collect to operate, improve and personalize the products and services we offer.

Customer Information will be used to provide the services and access to technology solutions you have purchased and the corresponding support.

We also may use the information to communicate with you, for example, informing you about your account and security updates.

And we may use the information to help make the ads you see on our ad- supported services more relevant.

3.2 Full text

AvePoint uses the information we collect to operate, improve and personalize the products and services we offer. Information collected through one AvePoint service may be combined with information collected through other AvePoint services to give you a more consistent and personalized experience in your interactions with us. We may also supplement this with information from other companies. For example, we may use services from other companies to help us derive a general geographic area based on your IP address in order to customize certain services to your geographic area.

We also may use the information to communicate with you, for example, informing you when a subscription is ending, letting you know when updates are available or letting you know when you need to take action to keep your account active. We may also use the information, if the law allows it or if we have your express permission to do so, to contact you for sales or marketing purposes.

We will use your Customer Information to:

- Provide the services and access to the technology solutions you have purchased;
- Renew subscription-based services;
- Provide customer support. While providing you with customer support we may also gather additional information from you to investigate technical issues, and respond to your support questions;
- Communicate regularly with you about your use of the software and service, AvePoint events and other industry or privacy-related news, and other AvePoint services we believe may be of interest to you. You may opt-out of receiving emails regarding AvePoint events and other AvePoint services by clicking unsubscribe link provided in the email. You will continue to receive notices regarding AvePoint software and technical services you purchased, and privacy-related updates such as notification of new or changes to existing privacy regulations

4. Reasons We Share Your Personal Information

4.1 Summary

Except as described in this privacy statement, we won't disclose your personal information to a third party without your consent.

Please see Other Important Privacy Information for details about when we may disclose information, including with AvePoint affiliates and vendors; when required by law or to respond to legal process; to combat fraud or protect our interest; or to protect lives.

4.2 Full text

Except as described in this privacy statement, we won't disclose your personal information to a third

party without your consent. Contexts and situations where we may disclose your personal data without your consent are:

- Within AvePoint affiliates and subsidiaries
- As part of a merger or sale of a business
- With vendors and agents of AvePoint
- When required by law or to respond to legal process or lawful requests, including from law enforcement or other government agencies or other public authorities, including to meet national security or law enforcement requirements
- When required to combat fraud or protect our interests
- To protect life and safety

Please also refer to section 11.2.2 to learn more about why and with whom we share or disclose personal information.

5. Accessing Your Personal Information

5.1 Summary

Some AvePoint services may give you the ability to view or edit your personal information online. To help prevent others from viewing your personal information, you first might be required to sign in. How you can access your personal information will depend on which sites or services you have used.

5.2 Full text

Some AvePoint services may give you the ability to view or edit your personal information online. To help prevent your personal information from being viewed by others, you first might will be required to sign in. The method(s) for accessing your personal information will depend on which sites or services you have used.

Each AvePoint web site may provide you with links to access, correct or delete your personal data. You can also contact AvePoint by using a provided contact form on the web site or by contacting the office of the General Counsel (see below for contact details). We will respond to requests to access or delete your personal information within 30 days.

Accessing and Updating your Personal Information

To review and update your personally identifying information to ensure it is accurate, contact us via email: privacy@avepoint.com

AvePoint will make commercially reasonable efforts to provide you reasonable access to any of your personal information we maintain within 30 days of your access request. We provide this access so you can review, make corrections, or request deletion of your data. If we cannot honor your request within the 30-day period, we will tell you when we will be able to provide access. In the unlikely event that we cannot provide you access to this information, we will explain why we cannot do so.

6. Children

6.1 Summary

When an AvePoint site or service collects age information, it will block users under 16 or obtain consent from a parent or guardian before their child can use it.

When consent is granted, the child's account is treated much like any other account, including being able to communicate with other users.

Parents can change or revoke consent as described in this privacy statement.

6.2 Full text

When an AvePoint site or service collects age information, it will either block users under 16 or will ask them to provide consent from a parent or guardian before they can use it. We will not knowingly ask children under 16 to provide more information than is necessary to provide the service.

When consent is granted, the child's account is treated much like any other account. The child may have access to communication services like e-mail, instant messaging and online message boards and may be able to communicate freely with other users of all ages.

6.3 Full Text

Parents can change or revoke the consent choices previously made, and review, edit or request the deletion of their children's personal information by using the contact form on the web site.

7. Communication Preferences

7.1 Summary

You can stop the delivery of future promotional e-mail from AvePoint sites and services by following the specific instructions in the e-mail you receive. Depending on the respective service, you may also have the option of proactively making choices about the receipt of promotional e-mail, telephone calls, and postal mail for particular AvePoint sites or services.

7.2. Full text

If you receive promotional e-mails from us and would like to stop getting them in the future, you can do so by following the directions in that message.

Depending on the respective service, you may also have the option of proactively making choices about the receipt of promotional e-mail, telephone calls, and postal mail from particular AvePoint sites or services by visiting and signing into the following pages:

These choices do not apply to the receipt of mandatory service communications that are considered part of certain AvePoint services, which you may receive periodically unless you cancel the service.

8. International Users - Applicable Law

8.1 Summary

Your personal information may be transferred to the United States or other countries. AvePoint transfers information to our corporate affiliates, service providers, and other partners who process it for us, based on our instructions, and in compliance with this policy and any other appropriate confidentiality and security measures. These partners provide us with services globally, including for customer support, information technology, payments, sales, marketing, data analysis, research and surveys.

8.2 Full text

Please note that the personal information you submit to us may be transferred to the United States and other countries to be processed by us in order to provide this Web Site, our technology solutions and services to you or for such other purposes as set forth in this Policy. AvePoint transfers information to our corporate affiliates, service providers, and other partners who process it for us, based on our instructions, and in compliance with this policy and any other appropriate confidentiality and security measures. These partners provide us with services globally, including for customer support, information technology, payments, sales, marketing, data analysis, research and surveys.

The transfer of personal data to other countries (including the United States) is protected by SCCs into which AvePoint has entered with all of its affiliated companies in order to ensure an adequate level of protection of such personal data. In addition to that, AvePoint has certified that it adheres to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Privacy Shield program, and to view AvePoint's certification, please visit <https://www.privacyshield.gov/>.

9. Support Data

9.1 Summary

Support Data is the information we collect when you submit a support request or run an automated troubleshooter, including information about hardware, software, and other details related to the support incident, such as: contact or authentication information, chat session personalization, information about the condition of the machine and the application from when the fault occurred and during diagnostics, system and registry data about software installations and hardware configurations, and error-tracking files. We use Support Data as described in this privacy statement, and additionally use it to resolve your support incident and for training purposes.

9.2 Full text

Support Data is the information we collect when you submit a support request or run an automated troubleshooter, including information about hardware, software, and other details related to the support incident, such as: contact or authentication information, chat session personalization, information about the condition of the machine and the application from when the fault occurred and during diagnostics, system and registry data about software installations and hardware configurations, and error-tracking files. We use Support Data as described in this privacy statement, and additionally use it to resolve your support incident and for training purposes.

Support may be provided through phone, e-mail, or online chat. We may use Remote Access (RA), with your permission, to temporarily navigate your desktop. Phone conversations, online chat sessions, or Remote Access sessions with support professionals may be recorded and/or monitored. For RA, you may also access the recording after your session. For Online Chat or RA, you may end a session at any time of your choosing.

Following a support incident, we may send you a survey about your experience and offerings. You must opt-out of support surveys separately from other communications provided by AvePoint, by contacting Support or through the e-mail footer.

To review and edit your personal information collected through our support services, please contact us by using our Web form.

Some business customers may purchase enhanced support offerings. These offerings are covered by their own contract terms and notices.

10. Payment Data

10.1 Summary

Payment Data is the information that you provide when you make purchases. This may include your payment instrument number (e.g., credit card, PayPal), your name and billing address, and the security code associated with your payment instrument (e.g., the CSV or CVV). This section provides additional information regarding the collection and use of your payment information.

10.2 Full text

Payment Data is the information that you provide when you make purchases. This may include your

payment instrument number (e.g., credit card, PayPal), your name and billing address, and the security code associated with your payment instrument (e.g., the CSV or CVV). This section provides additional information regarding the collection and use of your payment information.

Payment Data is used to complete your transaction, as well as for the detection and prevention of fraud. In support of these uses, AvePoint may share your Payment Data with banks and other entities that process payment transactions or other financial services, and for fraud prevention and credit risk reduction.

When you provide Payment Data to us, we may store that data to help you complete future transactions.

You may remove the payment instrument information associated with your organizational account by contacting us. After you close your account or remove a payment instrument, however, AvePoint may retain your payment instrument data for as long as reasonably necessary to complete your existing transaction, to comply with AvePoint's legal and reporting requirements, and for the detection and prevention of fraud.

11. Other Important Privacy Information

11.1 Summary

Learn more about

- Why and with whom we share or disclose personal information
- Protecting the security of personal information
- Where we store and process information
- Changes to our privacy statements
- How to Contact Us

11.2 Full text

Below you will find additional privacy information you may find important. Much of this describes practices that are common across the industry, but we want make sure you are aware of them. Please keep in mind that this information is not a complete description of our practices - this is all in addition to the other, more specific information contained elsewhere in this privacy statement.

11.2.1 On this page:

- Sharing or Disclosing Personal Information
- Protecting the Security of Personal Information
- Where Information is Stored and Processed
- Changes to Our Privacy Statements
- How to Contact Us

11.2.2 Sharing or Disclosing Personal Information

AvePoint transfers information to our corporate affiliates, service providers, and other partners who process it for us, based on our instructions, and in compliance with this policy and any other appropriate confidentiality and security measures. These partners provide us with services globally, including for customer support, information technology, payments, sales, marketing, data analysis, research and

surveys. In addition to any sharing described above in this privacy statement, AvePoint may share or disclose personal information:

- With other AvePoint controlled subsidiaries and affiliates.
- As part of a corporate transaction such as a merger or sale of assets.
- With vendors or agents. Specifically, we may share it with companies we've hired to provide services on our behalf. Examples of these services include analyzing data, providing marketing assistance, and processing credit card payments. When we share information with these other companies to provide services for us, they are not allowed to use it for any other purpose and must keep it confidential.

We also may share or disclose personal information, including the content of your communications:

- To comply with the law or respond to legal process or lawful requests, including from law enforcement and government agencies or other public authorities, including to meet national security or law enforcement requirements.
- To protect the rights or property of AvePoint or our customers, including enforcing the terms governing your use of the services.
- To act on a good faith belief that access or disclosure is necessary to protect the personal safety of AvePoint employees, customers or the public.

Please note that our sites may include links to third-party sites whose privacy practices may differ from those of AvePoint. If you submit personal information to any of those sites, your information is governed by the privacy statements on those sites. We encourage you to review the privacy statement of any site you visit.

11.2.3 Protecting the Security of Personal Information

AvePoint is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use or disclosure. For example, we store the personal information you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocols.

If a password is used to help protect your accounts and personal information, it is your responsibility to keep your password confidential. Do not share it. If you are sharing a computer, you should always log out before leaving a site or service to protect access to your information from subsequent users.

AvePoint has received ISO 27001:2013 certification with respect to secure software development and maintenance process including support business functions like Infosec, IT, HR, Sales and Marketing, Project Management, Operations and Call Center.

11.2.4 Where Information is Stored and Processed

Personal information collected on AvePoint sites and services may be stored and processed in the United States or any other country where AvePoint or its affiliates, subsidiaries or service providers maintain facilities. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located.

AvePoint may retain your personal information for a variety of reasons, such as to comply with our legal obligations, resolve disputes, enforce our agreements, and as long as necessary to provide services. To learn how to access your personal information, visit [Accessing Your Information](#).

11.2.5 Changes to Our Privacy Statements

We will occasionally update our privacy statements to reflect customer feedback and changes in our services. When we post changes to a statement, we will revise the "last updated" date at the top of the statement. If there are material changes to the statement or in how AvePoint will use your personal information, we will notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification. Material Changes must be agreed to in writing by and between AvePoint and Customer. We encourage you to periodically review the privacy statements for the products and services you use to learn how AvePoint is protecting your information.

11.2.6 How Can I Exercise My Data Subject Rights?

If you would like to access, review, update, rectify, and delete any Personal Information we hold about you, or exercise any other data subject right available to you under the EU General Data Protection Regulation (GDPR), please submit a written request by e-mail to: privacy@avepoint.com.

Our privacy team will examine your request and respond to you as quickly as possible.

Please note that we may still use any aggregated and de-identified Personal Information that does not identify any individual and may also retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Under the California Consumer Privacy Act (CCPA), California residents are entitled to ask us for a notice identifying the categories of Personal Information which we share with our affiliates and/or third parties for marketing purposes, and for us to provide contact information for such affiliates and/or third parties.

If you are a California resident and would like a copy of this notice, please submit a request via AvePoint's toll-free CCPA hotline number:

1-888-995-1342;

by e-mail to: privacy@avepoint.com; or

by mail to: AvePoint, Inc., River Front Plaza, West Tower, 901 East Byrd Street, Suite 900, Richmond, VA, Attn: General Counsel.

If you are a resident of the European Economic Area (EEA), please see the section below for users in the European Economic Area for further information about your privacy rights.

11.2.7 How to Contact Us and Ways to Resolve Disputes

- If you have a technical or general support question, please

visit <https://www.avepoint.com/> to learn more about AvePoint Support offerings.

- If you have a general privacy question, or a question with regards to this Privacy Policy, please contact AvePoint's Office of the General Counsel

by e-Mail to: privacy@avepoint.com; or

by mail to: AvePoint, Inc., River Front Plaza, West Tower, 901 East Byrd Street, Suite 900, Richmond, VA, Attn: General Counsel.

- If you are a resident of the EEA and have an unresolved privacy or personal information collection, use, or disclosure concern that we have not addressed satisfactorily, please contact the EU Data Protection Authorities. If you are a resident of Switzerland and have this concern, please contact the Swiss Federal Data Protection and Information Commissioner.

- For more information on how to contact the EU Data Protection Authorities, click here (http://ec.europa.eu/justice/dataprotection/article-29/structure/data-protectionauthorities/index_en.htm).

- For more information on how to contact the Swiss Federal Data Protection and Information Commissioner, click here (<https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/contact.html>).

EU-U.S. and Swiss-U.S. Privacy Shield

AvePoint adheres to the principles of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks, although AvePoint does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of personal data in light of the judgment of the Court of Justice of the EU in Case C-311/18. To learn more, visit the U.S. Department of Commerce's Privacy Shield website.

Accessing and Updating your Personal Information

- To review and update your personally identifying information to ensure it is accurate, contact us via email: privacy@avepoint.com

- AvePoint will make commercially reasonable efforts to provide you reasonable access to any of your personal information we maintain within 30 days of your access request. We provide this access so you can review, make corrections, or request deletion of your data. If we cannot honor your request within the 30-day period, we will tell you when we will be able to provide access. In the unlikely event that we cannot provide you access to this information, we will explain why we cannot do so.

- To find the AvePoint subsidiary in your country or region, see <https://www.avepoint.com/about/contact/>.

- For more information about Data Protection, Privacy and Security at AvePoint, please visit <https://www.avepoint.com/company/privacy-and-security/>.

Appendix B

AvePoint's Data Protection and Information Security Policy

<https://www.avepoint.com/agreements/dataprotection>

THIS DATA PROTECTION AND INFORMATION SECURITY POLICY represents the core information security policies and procedures for AvePoint, as it pertains to our treatment of customer data. Our information security program is a structured approach to develop, implement, and maintain an organizational environment that is conducive to appropriate information security, and it is AvePoint's goal that all customer interactions reflect our respect for information privacy and our commitment to transparency in communication.

1. How AvePoint Categorizes Data

1.1 AvePoint Data Categories and Definitions

Administrator Data

Is the information about administrators supplied during signup, purchase, or administration of AvePoint services, such as names, phone numbers, and email addresses. It also includes aggregated usage information and data associated with your account, such as the controls you select. We use administrator data to provide services, complete transactions, service the account, and detect and prevent fraud.

Customer Data

Is all data, including all objects and containers that reside in customer's environments. Customer Data includes, for example, SharePoint site collections, lists and libraries, or Exchange mailboxes, as well as customer content, which is a subset of Customer Data that includes, in part, Exchange Online email body and attachments, SharePoint Online site file content, and IM conversations.

Configuration Data

Is information provided by you, or on your behalf, that is used to identify or configure application, such as backup settings, service requests, as well as object/container scopes, but does not include their content or user identities. Examples of Configuration Data include the site collection URLs, admin user IDs, service requests (and their metadata such as requestor, template and settings, as applicable). Customers should not include Personal Data or other sensitive information in object metadata because object metadata may be shared across global AvePoint systems to facilitate operations and troubleshooting.

Account and Payment Data

Is data that AvePoint collects to maintain a business relationship with you. This includes the information you provide when making purchases with AvePoint. AvePoint does not process credit card payments directly, and all credit card payments are processed by a third party that is responsible for PCI compliance.

Personal Data

Means any information relating to an identified or identifiable natural person. In other words, Personal Data is any data that is associated with a specific person. Personal data provided by our customers through their use of our products and services, such as the names and contact information of customer end users, would also be Account and Payment data. But personal data could also include certain data that is not account and payment data, such as the user id our service assigns to each user; such personal data is considered pseudonymous because it alone cannot identify the individual.

Support and Consulting Data

Means all data, including all text, sound, video, image files, or software, that are provided to AvePoint by, or on behalf of, customer (or that customer authorizes AvePoint to obtain from an Online Service) through an engagement with AvePoint to obtain Professional Services or Support. This may include information collected over phone, chat, e-mail, or web form. It may include description of problems, files transferred to AvePoint to resolve support issues, automated troubleshooters, or by accessing customer systems remotely with customer permission. It does not include Administrator Data or payment data.

Data Storage and Location Matrix

	Data stored and encrypted by AvePoint? (Yes/No/NA)	Data accessible by AvePoint Employees? (Yes/No/NA)	Data storage location
Administrator Data	Yes , encryption provided by third party software	Yes , authorized personnel based on business needs	US – Based in Microsoft Dynamics data center
	Data stored and encrypted by AvePoint? (Yes/No/NA)	Data accessible by AvePoint Employees? (Yes/No/NA)	Data storage location
	NA , for on-premises and other AvePoint cloud applications		
Configuration Data	Yes , for cloud applications NA , for on-premises	Yes , for cloud applications, only by authorized support personnel when necessary during investigation customer initiated support case No , for on-premises	Customer selected data center
Account and Payment Data	Yes , encryption is provided by third party software	Yes , authorized personnel based on business needs	US – Based in Microsoft Dynamics data center
Support and Consulting Data	Yes , disk level encryption	Yes , only by authorized personnel when necessary during investigation customer initiated support case or services	A combination of Azure, AWS and local servers at AvePoint offices.

Note 1: Cloud applications that are backup and archiving in nature (for example, Cloud Backup and Cloud

Archiving) will copy Customer Data to encryption-enabled Azure Storage located in the data center selected by customer, under instructions from customer's personnel. The stored backup data is further encrypted by application with keys unique to each tenant. No AvePoint employees can access the unencrypted content on the storage. In addition, customers have the option to use their own encryption key (BYOK) and their own storage (BYOS).

Note 2: In order to perform their intended functions, the cloud applications need to access the Application Tokens or Service Accounts authorized by customers. The Application Tokens and Service Account credentials are encrypted by the applications with AES 256 using keys unique to each customer. No AvePoint employees can access them. In addition, a Bring-Your-Own-Key (or BYOK) option is available to perform the encryption using customers' own keys.

General. When a customer tries, purchases, uses, or subscribes to AvePoint Products, or obtains support for or professional services with such products, AvePoint collects data to provide the service (including uses compatible with providing the service), provide the best experiences with our products, operate our business, and communicate with the customer. For example:

- When a customer engages with an AvePoint sales representative, we collect the customer's name and contact data, along with information about the customer's organization, to support that engagement.
- When a customer interacts with an AvePoint support professional, we might collect device and usage data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When AvePoint sends communications to a customer, we use data to personalize the content of the communication.
- When a customer engages with AvePoint for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

1.2 How AvePoint Manages Data

You Own Your Data

Customer Data is only used to provide agreed upon services and if you leave the service, we take the necessary steps to ensure the continued ownership of your data.

Where Your Data Is Located

The data location depends on the specific nature of the data as outlined in the Data Storage and Location Matrix.

1.3 Who Has Access To Data

You do! We take strong measures to help protect Customer Data from inappropriate access or use by unauthorized persons, either external or internal, and to prevent customers from gaining access to one another's data. AvePoint operations and support personnel are located around the globe to help ensure that appropriate personnel are available 24 hours a day, 365 days a year. We have automated a majority of our service operations so that only a small set requires human interaction. More details are available in the Data Storage and Location Matrix.

2. Privacy and Information Security

2.1 Information Security

AvePoint will perform and provide the Services to our customers in such a manner so as to minimize the threat of unauthorized access to confidential information. AvePoint has implemented and maintains a comprehensive, written information security program that contains administrative, technical and procedural measures and physical safeguards designed to protect the security and confidentiality of confidential information, and to protect against any anticipated threats or hazards to the security and integrity of such information. AvePoint utilizes appropriate security measures, including: (i) encryption during the transmission or storage of customer provided data at all times, to the current national recognized industry standards, such as the Advanced Encryption Standard (AES 256); (ii) maintaining an intrusion and vulnerability management program; (iii) centrally managed and automatically updating anti-malware technology; (iv) tracking and monitoring of all access to network resources; and (v) appropriate technological measures to prevent data leakage.

2.2 Security Assessment

At least annually, AvePoint will perform a security assessment of the Services. The security assessment will include, but is not limited to: (i) an ISO 27001:2013 certificate or equivalent; (ii) a web application assessment of the public-facing system or website; and (iii) a summary of its vulnerability testing.

2.3 Security Logging and Monitoring

If applicable, tenant level audit logs will be available to customers, which can be exported by the customer at its convenience. The tenant level audit logs will contain, as applicable, the following:

- User account information;
- Time stamps; and
- Operation actions performed by users

2.4 Configuration and Change Management

AvePoint has a documented and functional configuration and change management process which includes testing of all changes in production environments and documented approval process of changes.

2.5 Security Awareness Training

AvePoint also has a documented mandatory information security training and security awareness program. This includes general awareness training for all employees as well as role-specific training.

2.6 Secure Coding

AvePoint follows a set of secure coding guidelines such as the OWASP secure coding guidelines.

2.7 Incident and Breach Response Program

AvePoint has in place an incident response program to mitigate, detect and respond to security incidents which includes the tools to find, eliminate or isolate the cause of any such security incident.

2.8 Multi-Factor Authentication

AvePoint employs a multi-factor authentication (as supported) for administrative access to any AvePoint systems supporting customer applications or systems.

2.9 Third Party Vendors

AvePoint's third party vendor risk assessment program requires vendors to participate in an information security and privacy, GDPR, and due diligence and compliance risk assessment questionnaire, which includes reviews of security certifications such as SOC II, type 2 or equivalent certifications.

2.10 Separation of Duties

AvePoint has appropriate separation of duty (SOD) controls implemented for all system administration user roles that manage Customer's Client Data or confidential information. All SOD are configured for least privilege to limit AvePoint's access to customer information and will ensure that no single person has the ability to manipulate the hardware, software, or processing of the Services to commit fraud or perform unauthorized actions without the oversight of another person.

2.11 Access Review

At least annually, AvePoint conducts a review and validation of its systems users' accounts to ensure the continued need for system access.

2.12 Security Policy

AvePoint has implemented, and maintains, a comprehensive set of security policies that satisfies the requirements set forth herein.

AvePoint reviews its security policies regularly, and particularly following any changes in applicable law, advances in technology or changes to AvePoint's information systems, in order to verify that the security policies and controls set out therein remain accurate, comprehensive and up to date.

2.13 Standards of Protection

AvePoint strives to secure and protect Customer Data by using at least the same degree of care as AvePoint uses to secure and protect its own confidential and proprietary information, and we work to ensure that in no event is Customer Data treated with anything less than reasonable care.

2.14 Risk Assessments and Mitigation

AvePoint performs regular (at least annually), comprehensive risk assessments with regard to data and business assets (e.g., facilities, equipment, devices, etc.), business processes, the threats against those assets and processes (both internal and external), the likelihood of those threats occurring and the impact upon the organization to determine an appropriate level of Information Security safeguards.

AvePoint manages, controls, and mitigates any risks identified in the Risk Assessment that could result in unauthorized access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of any Customer Data.

2.15 Organizational Security

Responsibility – AvePoint assigns responsibility for information security management to appropriate skilled and/or senior personnel only.

'Need to Know' Access – AvePoint restricts access to information systems used in connection with the services provided under each applicable customer agreement and/or to Customer Data to only those personnel who have sufficient technical expertise

for the role assigned and know his or her obligations and the consequences of any security breach.

Confidentiality – AvePoint personnel who have accessed or otherwise been made known of Customer Data maintain the confidentiality of such information.

2.16 Asset Management

Data Sensitivity – AvePoint acknowledges that it understands the sensitivity of the Customer Data.

Configuration Management – AvePoint has established a configuration baseline for all information systems using suitable knowledge resources, including applicable information security standards, manufacturer recommendations, and industry best practices. AvePoint has established appropriate monitoring to ensure that its information systems are configured in accordance with the established configuration baseline throughout the life of the information system.

2.17 Communications and Operations Management

Penetration Testing – On at least an annual basis, AvePoint will conduct a penetration test of AvePoint's products.

Data Encryption – As applicable, AvePoint encrypts or protects by other technical means Customer Data in AvePoint's possession or control so that it cannot be read, copied, changed or deleted by unauthorized personnel while in storage, including when saved on removable media. FIPS 140-2 Level 3 or ISO 19790 Level 3 compliant or equivalent encryption is required for certain data based on Customer determination.

Data Protection During Transmission or Transit – As applicable, AvePoint encrypts using an industry recognized encryption algorithm and protects Customer Data in AvePoint's possession or control so that it cannot be read, copied, changed or deleted by unauthorized personnel during transmission or transit inside or outside of AvePoint's internal network.

Network Ports – AvePoint restricts unauthorized network traffic to the environment that may process Customer Data.

Wireless Network – AvePoint ensures use of WiFi (aka 802.11) network traffic is encrypted using WPA2 with the AES encryption algorithm option and mutual authentication between the server and the end devices when accessing systems containing Customer Data.

Malicious Code – AvePoint detects the introduction or intrusion of malicious code on information systems handling or holding Customer Data and at no additional charge to customer, prevents the unauthorized access, disclosure or loss of the integrity of any Customer Data, and removes and eliminates any effects.

2.18 Access Control

Authorized Access – AvePoint maintains the logical separation such that access to all internal systems used by AvePoint that host the business relationship data that is used to provide services to customer will uniquely identify each individual requiring access, and grant access only to authorized personnel based on the principle of least privileges.

User Access Inventory – AvePoint maintains an accurate and up to date list of all personnel who have access to these systems and will have a process to promptly disable within twenty-four (24) hours of transfer or termination access by any individual personnel.

Authentication Credential Management – AvePoint communicates authentication credentials to users in a secure manner, with an appropriate proof of identity check of the intended users. Passwords are not be stored or transmitted in readable form.

Logging & Monitoring – AvePoint logs and monitor all access to these information systems for additions, alterations, deletions, and copying.

Multi-Factor Authentication for Remote Access – AvePoint uses multi factor authentication and a secure tunnel when accessing systems containing Customer Data remotely.

Multi-Factor Authentication for Internet Facing Applications – AvePoint requires multi- factor authentication for all users of Internet facing applications which permit financial instructions/transactions or display personally identifiable information.

2.19 Use of Laptops and Mobile Devices

Encryption Requirements – AvePoint encrypts any laptops or mobile devices (e.g., phones) containing Sensitive Customer Data used by AvePoint’s personnel using an industry recognized encryption algorithm with at least 256 bit encryption AES (or equivalent).

Secure Storage – AvePoint requires that all laptops and mobile devices be securely stored whenever out of the personnel’s immediate possession. In the event of a lost or stolen laptop or other mobile device containing Customer Data, AvePoint shall promptly notify customer.

Network/ Systems Password Storage – AvePoint prohibits use of laptops or other mobile devices (e.g., phones) to store network or system passwords that enable access to Customer systems or other systems that handle or hold Customer Data, unless such passwords are encrypted.

Remote Wipe/Inactivity Timeout – AvePoint employs access and password controls as well as inactivity timeouts of no longer than thirty (30) minutes on all laptops, desktops and mobile devices used by AvePoint’s personnel and maintains the ability to immediately upon knowledge remotely remove Customer Data from any mobile device lost, stolen or in possession of a terminated personnel.

Laptops/Mobile Devices – AvePoint prohibits access to Customer Data on laptops or mobile devices where the above requirements cannot be met.

2.20 Information Systems Acquisition Development and Maintenance

As shown in the above Data Access and Storage matrix, AvePoint employees do not have access to Customer Data. If applicable (e.g. for AvePoint’s Cloud Backup product), Customer Data will be processed by the AvePoint application solely for the purposes specified in each applicable agreement with a customer. Additionally, the following shall apply:

- No customer production data is used for any other purpose (e.g., QA testing, development testing, User Acceptance Test areas (UAT), training, demonstration, etc.).
- The production environment is a separate environment from any other non- production environment (e.g., development, UAT, etc.).

Software Patching – AvePoint regularly updates and patch all computer software on systems that handle or hold Customer Data, with patching for vulnerabilities rated ‘critical’ or ‘high’ applied within thirty (30) days of patch availability, unless other controls have been applied that mitigate the vulnerability.

Virus and other Malware Management – AvePoint provides protection from viruses and other malware (e.g. spyware, etc.) to AvePoint’s systems that handle or hold Customer Data, using the most recently distributed version of software including virus signatures updated at least every twenty-four (24) hours.

2.21 Incident Event and Communications Management

Incident Management/Notification of Breach – AvePoint has developed and implemented an incident response plan that specifies actions to be taken when AvePoint suspects or detects that a party has gained unauthorized access to Customer Data or systems or applications containing any Customer Data (the “Response Plan”).

The Response Plan includes:

- Incident Reporting – AvePoint will strive to promptly furnish to customer full details that AvePoint has or may obtain regarding the general circumstances and extent of such unauthorized access, including without limitation, the categories of Customer personal data and the number and/or identities of the data subjects affected, as well as any steps taken to secure the Customer Data and preserve information for any necessary investigation.
- Investigation & Prevention – AvePoint uses reasonable efforts to assist customer in investigating or preventing the reoccurrence of any such access and strives to
 - (i) cooperate with the customer in its efforts to comply with statutory notice or other legal obligations applicable to customer or its clients arising out of unauthorized access or use and to seek injunctive or other equitable relief; and
 - (ii) promptly take all reasonable actions necessary to prevent a reoccurrence of and mitigate against loss from any such unauthorized access.
- Personnel Training and Confidentiality – AvePoint has robust policies and procedures in place to ensure that all personnel fully understand the process and conditions under which they are required to invoke the appropriate incident response. AvePoint maintains strict confidentiality regarding actual or suspected unauthorized possession, use or knowledge of Customer Data or any other failure of AvePoint’s security measures or non-compliance with its security policies or procedures.

2.22 Limited Access

With respect to any AvePoint personnel who no longer requires, or is no longer authorized for whatever reason to have, access to Customer Data, where access is managed by customer, AvePoint will strive to so notify customer in writing at least twenty-four (24) hours prior to the date on which such access is no longer required or authorized; unless such access is removed under exigent circumstances such that twenty-four (24) hours prior notice is not possible in which case AvePoint will notify customer immediately upon knowledge that such access is being removed.

Notwithstanding the above, AvePoint will immediately terminate access to customer systems and premises by any AvePoint personnel who is either removed or is no longer actively engaged in any customer assignment or if such personnel ceases to be an employee. All customer assets including any equipment, documentation or information will be returned upon the termination of their assignment with customer.

AvePoint strives to:

- Promptly notify customer if AvePoint identifies a gap in the security measures implemented by customer;
- Promptly provide customer with information regarding any failure of Customer’s security measures or any security breach related to Customer Data that AvePoint becomes aware of in connection with its performance of the services at customer’s facilities; and
- Maintain confidentiality towards third parties regarding any such failure of such security measures or any security, subject to legal disclosure obligations.

Customer resources, including computers, software, proprietary information, and telecommunications equipment will not be used for any activity not related to customer business. All assigned mobile devices that connect to customer are in possession of AvePoint’s Personnel at all times or kept in a secure location. The customer’s network will only be accessed through an approved connection (e.g., ASG, SSL VPN etc.).

In no event will any Customer Data be removed from customer's premises or its network by AvePoint without prior authorization. Additionally, AvePoint personnel are prohibited from the following activities:

- Initiating or facilitating any unauthorized attempts to access customer information assets,
- Storing or sending of Customer Data or intellectual property to personal email accounts or any other personal accounts including, but not limited to, cloud storage accounts, any public location, social media sites, help forums or blogs,
- Copying, downloading or storing of Customer Data or intellectual property to removable data devices unless authorized and the device has been encrypted and approved by customer,
- Sharing of customer credentials (user IDs and passwords) and/or tokens with anyone or the use of customer credentials for accounts other than customer.

3. Personnel Management, Privacy, and Compliance

3.1 Background Check and Security Clearance

AvePoint's assigned personnel comply with the customer's policies and rules, including those relating to facilities access, systems access operating standards and procedures, user identification and password controls, corporate information, security and data protection and privacy, as in effect and as communicated to and accepted in writing by AvePoint from time to time as a condition to being provided access to customer's premises, systems or Customer Data. AvePoint will not, and will ensure that AvePoint personnel do not, break, bypass, or circumvent, or attempt to break, bypass or circumvent, any security system of customer, or obtain, or attempt to obtain, access to any Customer Data other than as allowed by customer in compliance with this Policy.

AvePoint personnel assigned to perform the services or otherwise having access to Customer Data may, in AvePoint's sole discretion, be subject to appropriate pre- employment background investigations performed by or on behalf of AvePoint consistent with industry standards taking into consideration the confidential nature of the services to be performed and the risk and severity of damage to customer or others that might result from its personnel's negligence or wrongful conduct. Upon written request from customer and subject to applicable data protection restrictions, in its sole discretion, AvePoint will make available evidence (such as invoices for services) that the background investigations have been performed on such personnel.

3.2 Physical Security

Securing Physical Facilities – AvePoint maintains AvePoint internal systems in a physically secure environment that restricts access to only authorized individuals, detects any unauthorized access or access attempts, and reports incidents and non- conformance of security policy to management. A secure environment includes 24x7 security personnel governance or equivalent means of monitoring of controls for all relevant locations (including, without limitation, buildings, computer facilities, and records storage facilities).

3.3 Personal Data

Compliance – To the extent applicable, AvePoint will retain, handle, process, host, have access to and/or otherwise use any personal data contained within the Customer Data perform its obligations hereunder in a manner that complies with all applicable laws, rules, regulations, ordinances, directives, decisions and codes, including, without limitation, relevant data protection and privacy laws.

Global Data Protection and Privacy – If and to the extent (i) AvePoint as a Processor processes Personal Data on behalf of customer as a Controller (as defined in Article 4 of the GDPR), and (ii) the customer is established within the EEA or Switzerland and/or to

the extent AvePoint Processes Personal Data of Data Subjects located in the EEA or Switzerland on behalf of customer or a customer affiliate, the Parties will comply with the terms of and complete and execute AvePoint's Data Processing Addendum ("DPA") for the purpose of ensuring that such Processing is conducted in accordance with applicable laws, including EU Data Protection Legislation (as defined within the DPA). Capitalized terms used in this section shall be defined in any applicable DPA, and capitalized terms used but not defined herein or in such DPA shall have the same meanings as set out in any applicable agreement between AvePoint and the customer.