PURECLOUD SERVICE TERMS AND CONDITIONS

This PureCloud Service Agreement and the documents referenced herein (**the "Agreement"**) contain terms and conditions that govern your access to and use of the PureCloud Service. The Agreement is entered into by You and Genesys Telecommunications Laboratories B.V., registered with the Netherlands Chamber of Commerce under the Business Register Number 24293219, with its corporate seat in Naarden, Netherlands and its business address at Gooimeer 6 – 02, 1411 DD Naarden, Netherlands (**"Genesys," "We," "Us," or "Our"**) and will allow You or the entity that You represent (**"You," "Your" or "Customer"**) to order PureCloud Services from Us. You

Agreement. The Agreement consists of this cover page, the Terms and Conditions, the PureCloud Schedule and any Services Orders and SOWs executed during the Term of this Agreement:

This Agreement constitutes the entire agreement and understanding of the parties relating to the subject matter hereof, superseding all prior or contemporaneous agreements, representations, promises and understandings, whether written, electronic, oral or otherwise. Except as expressly provided herein, each party acknowledges and agrees that by executing the terms and conditions specified in this Agreement, (i) it is not relying upon any other statements, representations, warranties, promises, assurances, or the like, (ii) no remedies are or will be available to a party with respect to the foregoing, and (iii) such remedies are unconditionally and irrevocably waived; provided, the foregoing shall not apply to any acts of fraud by a party.

This Agreement takes effect when both parties have executed the Services Order (the **"Effective Date"**). You represent to Us that You are lawfully able to enter into contracts that bind the entity You represent and that You have legal authority to do so.

TERMS AND CONDITIONS

SECTION ONE – SERVICES/DEFINITIONS

1.1 This Agreement contains general terms applicable to any Services that You purchase or license from Us. All Services will be identified in a Sevices Order or SOW and specific terms and conditions will apply.
1.2 In addition to the terms defined elsewhere in the Agreement, some defined terms that You should be familiar with are:

Affiliate: A business entity that: (a) Controls the party; (b) is Controlled by the party; or (c) is under common Control with the party, but only during the time that such Control exists. For the purposes of this definition, **"Control(led)"** is the ability to determine the management policies of an entity through ownership of a majority of shares or by control of the board of management.

Cloud Services: Our cloud service offerings as made available to You using equipment, facilities and software owned or operated by or for Us as further described in the applicable PureCloud Schedule.
Customer Data: Your proprietary information and information about your customers (including Personal Data) submitted through the Cloud Services by You or Your Users. Customer Data does not include Service Improvements as defined in 9.4.

Deliverables: means the configurations and modifications to the Cloud Services provided by Us to You pursuant to a Statement of Work.

Documentation means the end user manual(s) and other materials typically provided by Us for use with the Cloud Services, including applicable service descriptions found at https://help.mypurecloud.com/?p=8858.

Equipment: Third party products provided on a pass-through basis without warranty from Genesys.
Exclusions: the following conditions, which are deemed excluded from, and that terminate, Our warranty, defense or indemnity obligation: (i) use of Materials in combination with any non-Genesys equipment, software, services, processes, data or materials; (ii) Your non-compliance with this Agreement or Documentation; (iii) use of Materials after receipt of notice from Us to discontinue such use, including Your failure to use modifications provided by Us; (iv) the development or use of any alteration, derivation, modification or customization of the Materials; (v) Our compliance with Your requests or instructions or the use of any materials or data provided by You; (vi) Your business method(s) or process(es); or (vii) Your content or Customer Data or third party products.
Force Majeure: Delays or failures on performance resulting from acts beyond the control of a party. Such acts include acts of God, provider blockades, denial of service attacks, strikes, lockouts, riots, acts of war, terrorism, epidemics, Laws effective after the Effective Date, fire, communication line failures, power failures, earthquakes or other disasters natural or man-made.
Feedback: any suggestions, enhancement requests, recommendations, report, feedback, proposals, anonymized statistical data or other information concerning the Services. Notwithstanding anything to contrary herein contained, in no event shall Feedback be deemed Customer Intellectual Property unless such Feedback existed on or before the Effective Date.

Malicious Code: Viruses, worms, time bombs, corrupted files, Trojan horses and other harmful or malicious code, files, scripts, agents, programs, or any other similar code that may interrupt, limit, damage the operation of Genesys' or another's computer or property.
Personal Data: any information relating to Your customers that is protected by applicable privacy law.
Professional Services: the consulting and implementation services provided by Us relating to the Cloud Services and documented in a statement of work **("Statement of Work"** or **"SOW")** or Services Order.
Related Parties: A party's past, present and future officers, directors, employees, and other personnel, agents, insurers, reinsurers, servants, attorneys, parent company, subsidiaries and affiliates.
Services: the Cloud Services, Professional Services and Support.
Services Order: the document used to place orders for Cloud Services.
Support: the support and maintenance for the Cloud Services as described in the applicable PureCloud Schedule.
Term: the term of the Cloud Services selected, as set forth in the SOW or Services Order and as further described in the PureCloud Schedule.

SECTION TWO – SCOPE OF USE

2.1 **Proprietary Rights.** All trademarks, service marks, patents, copyrights, trade secrets and other intellectual property rights in any and all Services hardware, Documentation, Deliverables and any other materials, products or services provided to You or used in providing Services to You (collectively, **"Materials"**) are and shall remain the exclusive property of Genesys or its business partners, licensors or suppliers, as applicable, whether or not specifically recognized or perfected under applicable local law. Genesys and its business partners, licensors and suppliers reserve all rights not expressly granted in the Agreement and own all rights in all derivative works of the Materials and any copy, translation, modification, adaptation or derivation (including any improvement or development) of the Materials.

2.2 **Use of Materials and Services.** You will not, and will not permit or authorize any third party to: (a) sell, rent, lease, sublicense or otherwise make the Materials available to any third party except as expressly authorized by this Agreement; (b) modify or create any derivative works, functionally equivalent works, or translations of the Materials; (c) copy any feature, design or graphic in, or disassemble, reverse engineer or decompile the Materials or remove or modify any proprietary markings or restrictive legends placed on any Materials; (d) access or use the Materials to compete with Us or to assist anyone else to compete with Us; (e) remove or modify any proprietary markings or restrictive legends placed on any Materials; (f) take any action that jeopardizes Our rights or the rights of Our business partners, licensors or suppliers in any Materials; (g) violate any law, regulation, mandate or court order; (h) use the Materials in a manner that is defamatory, harassing, infringing or otherwise causes damage or injury to any person or property; (i) transmit viruses or other deleterious code; or (k) damage, disable, overburden or impair the Materials or any other party's use of the Materials. You are responsible for any use of the Materials by your Affiliates. You or any of Your end users shall not and shall not attempt to: (i) license, sell, lease or otherwise make the Services, or any like service, available to non-subscribers; (ii) use the Services in a way that violates any law, regulation or mandate, or the terms of this Agreement; or (iii) take any action that jeopardizes Our Confidential Information or proprietary information or acquire any right in the Services or in anything else shared with or made available to You. In addition, unusually high usage of the Services may impair Our ability to provide high quality services to others and/or indicate unauthorized use of the Services, in which case We may suspend or terminate Your use. You acknowledge and agree that You alone decide the content and timing of your telephone calls.

2.3 **Similar Materials and Services.** Subject to the confidentiality provisions of this Agreement, nothing in this Agreement precludes or limits Us in any way from providing materials or services that are similar to materials or services provided or contemplated in this Agreement or developing deliverables or other materials or services that are similar to or compete with any materials or services developed as a result of this Agreement, regardless of their similarity to any Materials, including Deliverables. We are free to use any concepts, processes, techniques, improvements or other know-how developed by Us in the course of performance of this Agreement (even if similar to materials, products and services provided hereunder) free from any use restriction or payment obligation. For the avoidance of doubt, but subject to this Agreement, including this Section 2.3, We do not claim any rights to Your Confidential Information.

2.4 **Cloud Services License**. We grant You and Your Affiliates a non-exclusive, non-transferable, worldwide right, limited to the Term, to authorize individuals solely within Your and Your Affiliates' organization to access the Cloud Services during the term of a Sevices Order but only for Your own internal business purposes and subject to the terms and conditions of this Agreement, the applicable service descriptions found at https://help.mypurecloud.com, the applicable PureCloud Schedule, the Documentation and the terms associated with the specific Services Order.

2.5 **Deliverables License.** You are granted a license to use Deliverables solely in connection with, and under the same provisions as, Your use of the Services.

2.6 To the extent not already owned by Genesys and subject in each case to Section 10.1 to the extent Customer is identified by name or logo, Customer, on behalf of itself and its Related Parties, hereby grants Genesys a perpetual, exclusive, royalty-free, worldwide license to use or disclose (or choose not to use or disclose), and create derivative works of Feedback for any purpose, in any way, in any media worldwide.

SECTION THREE – CONFIDENTIALITY

3.1 For purposes of this Agreement, the party disclosing Confidential Information is referred to as the **"Discloser"** and the party receiving Confidential Information is referred to as the **"Recipient." "Confidential Information"** means proprietary information of Discloser, or third party proprietary information disclosed to Discloser, that is provided to Recipient. Recipient's obligations to protect Discloser's Confidential Information does not apply to information that: (i) is or becomes, through no act or omission of Recipient, publicly available; (ii) is known by Recipient at the time of receipt, as shown by Recipient's contemporaneous written records; (iii) is subsequently and rightfully provided to Recipient by a third party, without restriction on disclosure; or (iv) is independently developed by Recipient without use of or access to Discloser's Confidential Information. Our Confidential Information includes the Materials and technical information relating to the Materials. Customer Data, is not Confidential Information it being understood that the terms and conditions regarding the safeguarding of Customer Data as outlined in Section 9 will apply to Customer Data.

3.2 Recipient will safeguard the confidentiality of Discloser's Confidential Information, including at a minimum, the precautions taken by Recipient to protect its own Confidential Information but in any event no less than reasonable precautions. Recipient will: (a) not disclose or use Discloser's Confidential Information for any purpose other than as contemplated by, and consistent with, the terms of this Agreement, (b) limit access to Discloser's Confidential Information only to its employees and agents who have a need to know such information and who are bound by written confidentiality obligations at least as protective as the requirements of this Agreement, and (c) not sell, transfer, disclose or otherwise make available Discloser's Confidential Information to any third party without the other party's prior written consent. If Recipient is required to disclose Discloser's Confidential Information under the terms of a subpoena, court order, governmental rule or regulation or other judicial requirement, unless legally prohibited from doing so, Recipient will promptly notify Discloser of the existence, terms and circumstances surrounding such a request or requirement so that Discloser may seek an appropriate protective order. If Discloser seeks a protective order, Recipient will reasonably cooperate in such effort at Discloser's expense. Subject to Recipient's compliance with the foregoing notice and cooperation obligations, Recipient will be allowed to make the required disclosure.

3.3 The Recipient will return any tangible materials containing Confidential Information, and any copies or reproductions thereof, to the Discloser within thirty (30) days after the Discloser's written request. Recipient agrees to undertake whatever action is reasonably necessary to remedy any breach of Recipient's confidentiality obligations or any other unauthorized disclosure or use of the Confidential Information by Recipient, its employees, its agents, or contractors. The Recipient acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information and that the Discloser Party shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction without the necessity of posting any bond.

SECTION FOUR – PAYMENT, TAXES AND RECORDS

4.1 **Cloud Services.** You will pay all fees and charges for Cloud Services pursuant to the applicable PureCloud Schedule and Services Order. Upon execution by both parties, each Services Order shall be a non-cancelable, non-refundable order by Customer. Subject to Section 4.6, We reserve the right to suspend the Cloud Services, or portion thereof, or reject or cancel the transmission of any information through the Cloud Service based upon (i) reasonable belief that the use of the Cloud Services is in violation of applicable Laws, (ii) Your failure to pay amounts when due, or (iii) an imminent compromise to the security or integrity of the network. As practicable depending on the circumstances, We will provide notice of the suspension and keep You reasonably informed of Genesys' efforts to restore the Cloud Services. Each year within a specified Term requires payment in exchange for the continued use of Cloud Services. You acknowledge and agree that fees quoted in a Sevices Order are contingent upon the agreed upon length of the entire multi-year Term. **These fees are not subject to early termination or cancellation and this obligation may not be waived.**

4.2 **Timing, Payment Disputes and Taxes.** All invoices for Services are due and payable within thirty (30) days of receipt unless otherwise set forth in the Services Order. Unless otherwise agreed, You shall pay all amounts due hereunder via Automated Clearinghouse (ACH), wire, or using Our E-bill portal, if applicable. We shall provide invoices electronically via email to a provided email address. If an invoicing portal is used, it shall be provided at the time the order is placed with Us. Subject to Section 4.3, all past due payments will bear interest at the rate of 1.5% or such lower rate as is required by law. You will pay any late payment charge upon remitting the principal amount to Us and will pay all collection costs incurred by Us. If any undisputed, invoiced amounts are more than thirty (30) days overdue then We may immediately suspend your use of the Cloud Services. Except as otherwise specified in the Services Order, the fees do not include any taxes. You are responsible for paying all taxes, levies, including any universal service fees, duties, or similar items, including any value-added, sales, use or withholding taxes other than taxes on Our net income **(collectively "Taxes")** associated with the Services Order and reimbursing Us for any Taxes with respect to the amounts due under any Services Order. If You are required to withhold Taxes from amounts payable to Us, You will timely remit it to the appropriate governmental authority in accordance with applicable laws and You will promptly furnish Us with the official receipt of payment of such Taxes to the appropriate taxing authority. You will not rely on Us to determine taxability and You are ultimately responsible for assessing and paying any applicable Taxes. If You provide us with an incorrect ship-to address or, where applicable, You do not provide Us with a valid tax exemption certificate prior to placing an Order, We will not provide you with a credit for such Taxes and You will be responsible for getting a refund from the applicable tax authority.

4.3 **Fee Disputes.** If You in good faith dispute the amount of any invoice, You will timely pay the undisputed amount and will notify Us in writing of the disputed amount no later than the date payment would otherwise be due, providing the reasons for the dispute. The

parties will attempt in good faith to resolve the dispute within thirty (30) days after Our receipt of Your notice of dispute **(the "Resolution Period")**, during which time withholding of the disputed amount will not be considered a material breach of this Agreement, no interest will accrue for late payment of the disputed amount. Upon resolution of the dispute, You will pay the resolved amount promptly but in any case within ten (10) days of mutual written agreement resolving the dispute. If the dispute is not resolved within the thirty-day (30) Resolution Period, then each party will be entitled to pursue all available remedies.

SECTION FIVE – PROFESSIONAL SERVICES

5.1 Professional Services. If applicable, We will provide the Professional Services identified in a Services Order or SOW executed by the parties.

SECTION SIX – WARRANTIES

6.1 Cloud Services Warranty. Beginning on the date that the term of the initial Services Order for Cloud Services commences, We warrant to You that the Cloud Services will materially conform to the then current description of the Cloud Services in the Documentation. If You become aware of a warranty breach, You must notify Us in writing. Your sole and exclusive remedy for breach of this warranty shall be either: (i) allow Us to modify the Cloud Services to conform to the current descriptions; or (ii) allow Us to provide a workaround solution that will reasonably meet your requirements. If neither option is commercially reasonable, We may terminate the Agreement and refund any pre-paid, unused fees.

6.2 Professional Services and Support Warranty. We warrant that the Professional Services and Support will be performed in a professional and workmanlike manner and in accordance with applicable requirements of this Agreement and any applicable SOW or Services Order. Your sole and exclusive remedy for breach of this warranty shall be for Us to re-perform non-conforming services.

6.3 DISCLAIMER. EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 6, WARRANTIES, ALL SERVICES AND OTHER MATERIALS OF ANY KIND, INCLUDING ANY AND ALL MATERIALS, THIRD PARTY PRODUCTS, DELIVERABLES, CUSTOMIZATIONS, HARDWARE, PROFESSIONAL SERVICES, SUPPORT SERVICES, AND CLOUD SERVICES, ARE PROVIDED "AS IS." TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, WE (AND OUR BUSINESS PARTNERS, LICENSORS AND SERVICE PROVIDERS) DISCLAIM ALL OTHER WARRANTIES, CONDITIONS, REPRESENTATIONS, INDEMNITIES AND GUARANTEES, WHETHER EXPRESS OR IMPLIED, ARISING BY LAW, CUSTOM, PRIOR ORAL OR WRITTEN STATEMENTS OR OTHERWISE (INCLUDING ANY WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, COMPATIBILITY, SECURITY, QUIET ENJOYMENT, TIMELINESS, COMPLETENESS OR ACCURACY). WITHOUT LIMITING THE FOREGOING, WE DO NOT WARRANT THAT USE OF ANY MATERIALS OR SERVICES WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ALL DEFECTS IN ANY SERVICES OR OTHER MATERIALS OF ANY KIND WILL BE CORRECTED. YOU ASSUME ALL RESPONSIBILITY FOR THE SELECTION OF THE SERVICES OR OTHER MATERIALS NECESSARY TO ACHIEVE YOUR INTENDED RESULTS. TO THE EXTENT THAT WE CANNOT DISCLAIM A WARRANTY AS A MATTER OF APPLICABLE LAW, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW.

6.4 WE SHALL HAVE NO WARRANTY OBLIGATIONS TO THE EXTENT A CLAIM AROSE FROM THE EXCLUSIONS. FURTHER, THE REMEDIES SET FORTH IN THIS SECTION SIX (WARRANTIES) ARE YOUR SOLE AND EXCLUSIVE REMEDY(IES) FOR ANY BREACH OF THE FOREGOING WARRANTIES AND TO THE EXTENT THAT ANY OTHER AGREEMENT BETWEEN US IS DETERMINED BY A COURT TO PROVIDE FOR A DIFFERENT REMEDY, THIS AGREEMENT SHALL CONTROL.

SECTION SEVEN – LIMITATION OF LIABILITY AND INDEMNIFICATION

7.1 CONSEQUENTIAL AND RELATED DAMAGES EXCLUSION. SUBJECT TO SECTION 7.3, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR:

7.1.1 ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, COVER DAMAGES, OR ANY OTHER SIMILAR DAMAGES WHATSOEVER;

7.1.2 ANY LOSS OF PROFITS, BUSINESS, GOODWILL (INCLUDING PECUNIARY LOSSES ARISING FROM LOSS OF GOODWILL), OR REVENUE, LOSS OR CORRUPTION OR DESTRUCTION OF DATA; AND/OR

7.1.3 ANY LOSS ARISING FROM THE TRANSMISSION OF VIRUSES.

7.2 LIMITATION OF LIABILITY. SUBJECT TO SECTIONS 7.1 AND 7.3, GENESYS' (AND ITS BUSINESS PARTNERS', LICENSORS' AND SUPPLIERS') TOTAL AGGREGATE LIABILITY ARISING IN CONNECTION WITH THE PEFORMANCE OR CONTEMPLATED PERFORMANCE OF THIS AGREEMENT, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR BREACH OF STATUTORY DUTY), MISREPRESENTATION, RESTITUTION OR OTHERWISE, WILL NOT EXCEED THE FEES PAID OR PAYABLE TO US IN THE TWELVE (12) MONTHS PRECEDING

THE CLAIM OR, IF THE CLAIM AROSE DURING ANY PERIOD BEFORE TWELVE (12) MONTHS HAD ELAPSED FROM THE EFFECTIVE DATE, DURING THAT SHORTER PERIOD, FOR THE MATERIALS OR SERVICES THAT ACTUALLY CAUSED THE LOSS, COST, CLAIM OR DAMAGE. CUSTOMER ACKNOWLEDGES AND AGREES THAT THIS LIMITATION ON LIABILITY FORMS A FUNDAMENTAL BASIS OF THE BARGAIN HEREUNDER, IN THE ABSENCE OF WHICH, THE ANNUAL TERM OF AND FEES PAYABLE UNDER OF THIS AGREEMENT WOULD HAVE BEEN DIFFERENT. THIS SECTION WILL NOT APPLY TO DAMAGES THAT CANNOT BE LIMITED OR EXCLUDED BY LAW (IN WHICH EVENT THE LIMITATION WILL BE THE MINIMUM AMOUNT REQUIRED BY LAW). **THIS SECTION AND OUR INDEMNIFICATION OBLIGATIONS TO YOU UNDER SECTION 7.3 REPRESENT YOUR SOLE AND EXCLUSIVE REMEDY FOR INFRINGEMENT CLAIMS ARISING IN CONNECTION WITH THIS AGREEMENT**.

7.3 **LIABILITY INCAPABLE OF EXCLUSION**. NOTHING IN THIS AGREEMENT EXCLUDES EITHER PARTY'S LIABILITY: (A) FOR DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE; (B) FOR FRAUD OR FRAUDULENT MISREPRESENTATION; (C) ANY OTHER LIABILITY WHICH CANNOT BE LIMITED OR EXCLUDED BY APPLICABLE LAW; OR (D) EITHER PARTY'S INTELLECTUAL PROPERTY OBLIGATIONS (AND IN THE CASE OF CUSTOMER, ITS OBLIGATIONS UNDER SECTION 2 (SCOPE OF USE).

7.3 **Genesys Indemnification.** Subject always to your compliance with Section 7.5 (Indemnification Procedures), We will pay to defend You at Our expense and indemnify You for any amounts awarded against You in a final judgment or settlement approved by Us, with respect to any claims by a third party that the unaltered Cloud Services, as originally delivered to You, infringe any patent, copyright or trade secret of such third party. If your use of the Cloud Services may infringe any third party intellectual property rights, we may at any time and at Our option and expense: (i) obtain for You a license to continue to use the Cloud Services that may infringe that third party's rights; (ii) modify the Cloud Services so as to avoid infringement while preserving substantially equivalent functionality; or (iii) terminate the Agreement and the licenses granted hereunder and refund to You the prepaid and unearned fees covering the remainder of the term of the applicable Services Order.

7.4 **Customer Indemnification.** You will defend Us and Our Affiliates at Your expense and indemnify Us and Our Affiliates against any judgments finally awarded by a court, and pay any settlements approved by You with respect to any claims: (a) that Customer Data and/or Your method or process of doing or conducting business infringes any intellectual property rights of a third party; (b) arising from Your non-compliance with the Agreement, including Section 2 (Scope of Use); or (c) any circumstances arising under the Exclusions.

7.5 **Indemnification Procedures.** A party entitled to indemnification (**"Indemnified Party"**) will promptly notify the other party (**"Indemnifying Party"**) of any claim and provide reasonable assistance to the Indemnifying Party with respect to handling the claim, at the Indemnifying Party's expense. Failure to provide timely notice or reasonable assistance will relieve the Indemnifying Party of its indemnification obligations to the extent that the Indemnifying Party has been materially prejudiced thereby. The Indemnifying Party will have the sole right to defend and settle any claim (except that the Indemnifying Party may not agree to any settlement that does not unconditionally release the Indemnified Party, without the Indemnified Party's prior written consent). The Indemnified Party will be entitled to participate in the defense of a Claim and to employ legal representation at its own expense to assist in the handling of a claim.

7.6 **WE SHALL HAVE NO DEFENSE, WARRANTY OR INDEMNIFCATION OBLIGATIONS TO THE EXTENT ANY CLAIM(S) AROSE FROM AN EXCLUSION(S).**

SECTION EIGHT – TERM AND TERMINATION

8.1 **Term**. The term of this Agreement shall begin on the Effective Date and shall continue during the term of all outstanding Services Orders and SOWs issued under this Agreement (the **"Term"**). Each Services Order shall indicate its term.

8.2 **Termination for Cause.** Either party may immediately, upon written notice to the other party, terminate the Agreement (i) if the other party breaches a material term of the Agreement (including, in the case of the Customer, any breach of the AWS Acceptable Use Policy) and (if such breach is remediable) fails to remedy that breach within thirty (30) days of being notified in writing to remedy the breach; and (ii) if the other is the subject of a bankruptcy order, or becomes insolvent, or makes any arrangement or composition with or assignment for the benefit of its creditors, or if any of its assets are the subject of any form of seizure, or goes into liquidation, either voluntary (otherwise than for reconstruction or amalgamation) or compulsory or if a receiver or administrator is appointed over its assets (or the equivalent of any such event in the jurisdiction of such other party. If You terminate this Agreement for cause, as your sole and exclusive remedy We will refund any pre-paid, unused fees for the Cloud Services.

8.3 **Effect of Termination**. Immediately upon termination, the licenses granted hereunder and rights to use shall terminate, and You must stop using the Materials. Within five (5) days after termination You will (a) return the Materials and all copies or (b) destroy the Materials and all copies, and confirm in writing that they have been destroyed. We will retain data for thirty (30) days (or such period as may be required by applicable law), during which time You may request a copy of Your data.

8.4 **Survival of Terms.** All terms of this Agreement which, by their nature, are intended to survive termination of this Agreement will survive termination, including all payment obligations, use restrictions, confidentiality obligations, ownership terms, customer data terms, warranty disclaimers, indemnification obligations, disclaimers, Exclusions and limitations of liability, effect of termination and general terms.

SECTION NINE – CUSTOMER DATA

9.1 As between Genesys and You, You retain ownership of and all intellectual property rights in Customer Data and grant Us a non-exclusive, non-sublicenseable (except to parties working on Our behalf), non-transferable, royalty-free license to access, process, store, transmit, and otherwise make use of the Customer Data as necessary to provide the Services and to otherwise fulfill Our obligations under the Agreement. Customer Data shall be processed in accordance with the attached Data Processing Schedule.

9.2 Our security and privacy policies, which are incorporated by reference, are located at https://help.mypurecloud.com/articles/purecloud-security-compliance/.

9.4 You may provide Customer Data for use with the Services. Notwithstanding Our obligations under the Data Processing Schedule, You are the only Data Controller (as defined in the applicable data protection law, including the Regulation (EU) 2016/679) of your Customer Data and You are solely responsible for the content and legal sufficiency of your Customer Data. We make no claim of ownership to Customer Data.

9.5 We will keep the Customer Data secure and confidential in accordance with the Data Processing Schedule, Section 3 (Confidentiality) of this Agreement and Our security and privacy policies. You confirm that You have notified any Data Subjects of, and that You have a lawful basis for, Our use of Customer Data to provide the Services to You, including Our use of AWS for storage of Customer Data in accordance with the AWS Customer Agreement.

9.6 You will ensure that You have appropriate security policies, including data archiving, in place and You are responsible for the distribution, ongoing management, maintenance, security and proper use of all valid usernames, userIDs and passwords used in connection with the Cloud Services.

9.7 We may aggregate data and information related to the performance, operation and use of the Cloud Services to create statistical analyses, to perform benchmarking, to perform research and development and to perform other similar activities (**"Service Improvements"**). We will not incorporate Customer Data in Service Improvements in a form that could identify You or Your customers and We will use industry standard techniques to anonymize Customer Data prior to performing Service Improvements. We retain all intellectual property rights in Service Improvements and may make them publicly available.

SECTION TEN – GENERAL

10.1 Marketing. Subject to prior written approval of content, You grant Us with the right to issue a media release after the Effective Date announcing that You have become a Genesys customer, and to make other announcements and place promotion in various publications and media. Except as set forth in a mutually agreed written public statement, You will not imply or state that You are affiliated with or endorsed by Us, publicize the existence of the Agreement, or disclose any of its terms. You also agree that, not less than once per calendar quarter during the Term, to act as a reference customer as requested by Us.

10.2 Assignment. Neither party may assign its rights or obligations under the Agreement, either in whole or in part, except (1) with respect to a sale of substantially all of the assets of its business, merger, or change in the party's ownership, (2) to an Affiliate or (3) with the prior written consent of the other party. Without limiting the preceding sentence, the rights and liabilities of the parties hereto shall bind and inure to the benefit of their respective successors and assigns. You understand and agree that third parties, including but not limited to Genesys' affiliates (e.g. Genesys Telecom US, Inc.) may provide products and services to You in connection with the Agreement. You agree that any such third parties may directly invoice You for services rendered and products delivered and You agree to pay such invoices.

10.3 Compliance with Laws. Each party will comply with all laws, statutes, rules, regulations, ordinances and other pronouncements having the effect of law **(collectively "Laws")** as applicable to a party and, in the case of Customer, applicable to the Materials and their use. In no event will We be responsible for providing, implementing, configuring, or coding the Materials in a manner that complies with any Laws that apply to Your business or industry, including without limitation, the Communications Act of 2003 as implemented by OFCOM, the UK Anti-Bribery Act, the Foreign Corrupt Practices Act, the FTC or FCC regulations or the Telephone Consumer Protection Act of 1991 **(collectively "Customer Specific Laws")**. You will comply with Customer Specific Laws, and in no event will We, Our business partners, licensors or suppliers be liable for any claim or action arising from or related to Your failure to comply with any Customer Specific Laws it being understood that You are solely liable for any such failure(s) and resulting claims or actions.

10.4 Anti-Corruption and Bribery Act Compliance. In connection with any actions or activities associated with this Agreement or in connection with the relationship between the Parties, neither Party shall engage in any unlawful trade practices or any other practices that are in violation of the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act of 2010, or any other law that prohibits bribery or similar activity. Each Party shall ensure that neither it nor its Affiliates, subcontractors and agents: either directly or indirectly, seek, receive, accept, give, offer, agree or promise to give any money, facilitation payment, or other thing of value from or to anyone (including but not limited to government or corporate officials or agents) as an improper inducement or reward for or otherwise on account of favourable action or forbearance from action or the exercise of influence; or fail to establish appropriate safeguards to protect against such prohibited actions. Each Party shall, upon request from the other Party, provide evidence of the steps being taken to avoid

prohibited actions, including the establishment of policies, practices, and/or business controls with respect to these laws. To the extent permitted by the relevant authority, each Party shall promptly inform the other Party of any official investigation with regard to alleged breaches of the above laws that are related in any way to this Agreement.

10.5 Cumulative Remedies, Force Majeure and Injunctive Relief. All remedies available to Us will be cumulative and the specification of a remedy will not preclude Us from pursuing other remedies available at law, or in equity. Neither party will be responsible for acts of Force Majeure. Nothing in this Agreement will prevent Us from seeking immediate injunctive relief against You in the courts having jurisdiction over You.

10.6 Governing Law. This Agreement shall be governed by the laws of England and Wales. The parties irrevocably agree that the courts of England and Wales have non-exclusive jurisdiction to settle any legal or equitable claim of any nature arising hereunder.

10.7 Independent Contractors. The parties are acting as independent contractors. Nothing in the Agreement shall be construed to create a partnership, joint venture or agency relationship between the parties.

10.8 Third party beneficiaries. No third-party beneficiary relationships are created by this Agreement.

10.9 Notices. All notices under the Agreement shall be in writing and shall be deemed to have been given when (a) personally delivered; (b) sent by electronic facsimile transmission; (c) sent by registered mail, postage prepaid (which notice shall be deemed to have been received on the third (3rd) business day following the date on which it is mailed); (d) in Our case, we may provide notice(s) of website modifications described in Section 10.12 by (i) posting a notice on our corporate website; or (ii) sending a message to the email address then associated with Your account; or (e) sent overnight by a commercial overnight courier that provides a receipt (which notice shall be deemed to be received on the next business day after mailing). In the case of Genesys, notice shall be sent to the address for the applicable Genesys entity at https://www.genesys.com/company/legal-docs/governing-law-jurisdiction-and-notices, with a mandatory copy to the attention of General Counsel, Legal, at the same address. In the case of Customer, notice shall be sent to the address below (or such other designee/address Customer may provide by giving notice to the in compliance with the Agreement).

10.10 Waiver. No provision of the Agreement may be waived unless such waiver is in writing and signed by the party against which the waiver is to be effective. Our failure to act with respect to a breach by You of this Agreement does not constitute a waiver of Our rights with respect to subsequent or similar breaches.

10.11 Severance. If any provision of this Agreement is deemed invalid, illegal, or unenforceable, it will be considered stricken from this Agreement, and the validity, legality and enforceability of the remaining provisions will not in any way be affected or impaired thereby.

10.12 Complete Agreement; Amendment. The Agreement constitutes the complete agreement between the parties and supersedes all prior agreements and representations, written or oral, concerning the subject matter of the Agreement. In the event of a conflict between the terms of a Sevices Order or SOW and the other provisions of the Agreement, the terms of the Agreement shall take precedence. The Agreement, other than as permitted under Section 10.13 (Modifications), may not otherwise be modified or amended except in a writing signed by a duly authorized representative of each party. The terms of the Agreement shall supersede the terms in any purchase order submitted by You or other ordering document..

10.13 Modifications. We may modify any websites referenced in the Agreement at any time by posting a revised version on the applicable Genesys websites or by otherwise notifying You in accordance with the Notice provisions in Section 10.9 (Notices). The modified terms will become effective upon posting or, if We notify You by email, as stated in the email message. By continuing to use the Services after the effective date of any modifications to the Agreement, You agree to be bound by the modified terms. If such modification materially decreases any of Our obligations or the functionality of the applicable Service, We will either obtain Your consent or You may terminate this Agreement by providing Us with written notice within thirty (30) days of the effective date of the applicable modification. Any such termination shall be effective thirty (30) days after We receive written notice from You.

10.14 Compliance. You represents and warrant that (a) neither You, any Affiliate, or any of Your users are on any government-issued list of restricted persons or entities including the Commerce Department Entity List, Denied Persons List or Unverified List, the Treasury Department Specially Designated Nationals and Blocked Persons List, and the State Department Debarred Parties List; and (b) You will not export or re-export, directly or indirectly, any services, products, Materials or confidential or proprietary information of any kind provided by Us to any countries outside the United States except as permitted under the U.S. Commerce Department's Export Administration Regulations. The products contain Commercial Computer Software under Federal Government Acquisition Regulations and agency supplements to them and are provided to the Federal Government and its agencies only under the Restricted Rights Provision of the Federal Acquisition Regulations applicable to commercial computer software developed at private expense and not in the public domain. **Execution; Digitized Copies.** The parties agree that this Agreement may be executed by any means of signature, including electronic commerce or transmission, including facsimile, email, or acknowledgement through a webpage. The Agreement may be executed in two (2) or more counterparts, each of which is deemed an original, but which together constitute one contract or document. Signed digitized copies of the Agreement and other associated documents, including attachments and amendments shall legally bind the parties to the same extent as original documents.

10.15 Subcontracting. We may subcontract certain portions of the Services under this Agreement to third parties, provided that We shall be responsible for the performance of such subcontractors.

10.16 Business Partners. Our benefits, rights, and obligations related to Scope of Use, Warranty Disclaimers, Customer Indemnification, Consequential and Related Damages Exclusion, Limitation of Liability, Confidentiality and Compliance with Laws shall extend to Our affiliates, related parties, business partners, licensors, and service providers.

10.17 Your users. You take full responsibility for ensuring that all of your personnel, third party service providers, and all other third parties that access or use the Services comply with this Agreement and You will be liable for their acts and omissions.

PURECLOUD SCHEDULE

This PureCloud Schedule contain terms and conditions that govern Your access to and use of the PureCloud Service (as defined below).

1. **Subscription Services.** We grant You a right to use the PureCloud Service in accordance with this Agreement and the applicable product descriptions found in the Services Order.
    1. The software used to provide the PureCloud Service is located on servers that are controlled by Amazon Web Services, Inc. ("**AWS**"). You may access and use the software but have no right to receive a copy of the object code or source code to the software.
    2. You shall comply with the AWS Acceptable Use Policy found at https://aws.amazon.com/aup/. You acknowledge that AWS may modify the AWS Acceptable Use Policy from time to time, and that, upon your renewal of the PureCloud Service, it is your responsibility to check the AWS Acceptable Use Policy for modifications to the policy. By continuing to use the PureCloud Service after renewal of the Agreement, You agree to be bound by the modified terms which are incorporated in the Agreement by this reference.
    3. PureCloud Edge Devices (**"Edge Devices"**), other third party components, and/or any professional services performed by third-parties may be made available to You by Our business partners in connection with your use of the PureCloud Service, and are provided "as-is". The terms and conditions governing the use of any such third-party products will be the terms of the shrink-wrap, click-wrap or other third-party license included with such products. We will pass through to You any warranties We receive from the supplier of such products, and to the extent such pass through is not allowed by the supplier, We will facilitate the filing of a warranty claim for any defective products. It is your responsibility to prepare and maintain the location where the hardware is installed so as to conform to any utility, climate control, wiring, networking and communication interface specifications, to perform all regular maintenance.
    4. In addition to third party products identified on a Services Order, You may also purchase third party products and services through Our AppFoundry website. You will be required to accept the supplier's terms and conditions through the AppFoundry website prior to activating your license to the AppFoundry product. Your use of the AppFoundry products is subject to such supplier terms and conditions, and not the terms and conditions of this Agreement. We are not a party to the terms and conditions of governing AppFoundry products, and all claims with respect to such AppFoundry products will be made with the supplier, and not Genesys. By activating an AppFoundry product, You are granting Us permission to share your PureCloud Services configuration and user information with the AppFoundry supplier, only to the extent such information is required by the AppFoundry supplier in order to provide the product.
2. **Security and Privacy**
    1. Our security and privacy policies for the PureCloud Service addressing use of Customer Data, which are incorporated by reference, are located at https://help.mypurecloud.com/articles/purecloud-security-compliance/.
3. **PureCloud Documentation.** The PureCloud Documentation is found at https://help.mypurecloud.com/articles/feature-list/, which is incorporated in the Agreement by this reference.
4. **Provision of PureCloud Service.** We will make the PureCloud Service available 24 hours a day, 7 days a week, except for: (i) occasional planned downtime at non-peak hours (for which We will provide advance notice); or (ii) any unavailability caused by circumstances beyond Our reasonable control, including failure or delay of your Internet connection, misconfiguration by You or any third party, issues on your network, or telecommunications services contracted by or for You, or (iii) unavailability as a result of the actions of AWS, including (a) any maintenance or planned downtime of the AWS services, (b) any fault or failure of the AWS services, or (c) AWS either terminating the AWS Customer Agreement or suspending Our or your use of AWS services. Your use of the PureCloud Service is subject to Our complete PureCloud Support Policies and Service Level Agreements (SLAs), which are provided at https://help.mypurecloud.com/articles/service-level-agreements/and are incorporated in the Agreement by this reference.
5. **Term and Payments.**
    1. **Term.** This Agreement governs use of the PureCloud Services starting on the Effective Date and continues until the end of the term of all Services Orders for PureCloud Services. The Initial Subscription Term shall begin after a period specified in the Services Order that is intended to allow You to implement the PureCloud Services (**"Ramp Period"**). The Ramp Period shall begin upon Our acceptance of the Services Order and shall be ninety (90) days if not otherwise specified in the Services Order. The Initial Subscription Term shall begin upon the end of such Ramp Period. At the end of the Initial Subscription Term, Services Orders for PureCloud Services shall renew on an annual basis (with an annual payment structure, as described below in 5.2.2.1), unless: (a) either party provides not less than 30 days' written notice of its intent to not renew; (b) the Services Order provides for a different automatic renewal period; or (c) the parties agree in writing to renew for a term of different duration. Pricing for any subsequent renewal period shall be at Our then current list pricing, unless otherwise agreed upon in a Sevices Order.
    2. **Payment Structure.** You must pay the fees listed on the relevant Services Order. Subscription payments will be structured differently based on the term You select from the three options below and the payment structure will be set forth in the

Services Order. The fees identified in the Services Order are exclusive of shipping fees, and You will pay the shipping fees (if applicable) identified in the invoice.

1. **Monthly Term**. The actual monthly fees will be calculated based on usage and invoiced to You in arrears on a monthly basis. Payment shall be due within thirty (30) days of the date of an invoice, unless the Services Order provides for a different payment term. Subscription prices for the monthly term are subject to changes in Our then current pricing. Note that subscription pricing for a monthly term is at a higher price than that for an annual term. During the Ramp Period, no monthly minimum shall apply. After the ramp period, there will be a monthly minimum that is set forth in the Services Order.
2. **Annual Term**.
    1. **Annual Pre-Payment.** Unless the applicable Services Order contains other payment terms, you will be billed in advance for twelve months of subscription fees. Unless the Services Order provides for a different payment term, such payment shall be due within thirty (30) days of the Effective Date, regardless of whether or not a Ramp Period applies. This payment covers the Term of the Agreement, beginning upon the end of the Ramp Period. During the Ramp Period, You will be billed for actual usage at the pro-rated Annual Subscription rates set forth in the Services Order. After the Ramp Period, if actual usage in a month exceeds Annual Subscription amount set forth in the Services Order (prorated for a one-month period), You will be charged for such excess usage at the Subscription Overage fee listed in the Services Order. All invoices are due within thirty (30) days of the date of such invoice, unless otherwise provided in the Services Order. Any prepaid amount is non-refundable.
    2. **Monthly Payment.** During the Ramp Period, You will be billed for actual usage at the monthly subscription rates set forth in the Services Order. Your monthly subscription fees will be set forth in the Services Order. After the Ramp Period, the monthly subscription represents a minimum billing amount. Any usage above the Monthly Subscription will be charged at the subscription overage fee listed in the Services Order.

6 <u>Definitions</u>.

1. **"AppFoundry"** means Our marketplace website where Customers may purchase third party software applications to integrate with the PureCloud Service.
2. **"PureCloud Service"** means Our cloud communications service, and associated equipment and services, as described in a Sevices Order.
3. **"PureCloud Website"** means the website used to access the PureCloud Service and any successor or related site designated by Us.
4. **"Initial Subscription Term"** means the initial term of the PureCloud Services You selected, as set forth in the Services Order.

GENESYS

Data Processing Schedule

1. **DEFINITIONS**
   a. ***In General.*** Capitalized terms used in this Data Processing Schedule ("DPS") but not defined herein shall have the meaning given to them in the Master Agreement or the Privacy Legislation.
   b. ***Affiliates*** means, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity;
   c. ***Customer Data*** means the personal data (as defined in the Privacy Legislation) that is uploaded to the Service.
   d. ***EEA*** means the European Economic Area.
   e. ***Master Agreement*** means the agreement executed by Genesys and the Customer for the provision of Services.
   f. ***Privacy Legislation*** means the Regulation (EU) 2016/679 (the "***General Data Protection Regulation***"), the Directive 2002/58/EC (ePrivacy Directive) and any further applicable national and international privacy and data protection legislations and regulations, as such legislations and regulations are amended, extended and re-enacted from time to time;

   g. ***Service(s)*** means the software, professional services, and customer care services provided by Genesys and further described in the Master Agreement.
   h. ***Standard Contractual Clauses*** means DPS Attachment 1 to this DPS, pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive 95/46/EC.

2. **DATA PROCESSING**
   a. ***Scope.*** This DPS governs the processing of Customer Data by Genesys. This DPS is intended to govern the data processing related to the Services in line with the Master Agreement. This DPS shall be coterminous with the Master Agreement.
   b. ***Compliance with Laws.*** Each party will comply with all laws, rules, and regulations applicable to it.
   c. ***Instructions for Data Processing.*** Genesys will process Customer Data in accordance with Customer's instructions, as set forth in this DPS and in the Master Agreement. To ensure compliance with its own data protection obligations pursuant to applicable Privacy Legislation, the Customer will first use the functions of the platform provided by Genesys. If Customer cannot redress an action required by applicable Privacy Legislation with those tools or functions provided by Genesys, Customer is entitled to give detailed instructions to Genesys. The Customer shall immediately confirm oral instructions regarding privacy either via a support care ticket or an email to DataPrivacy@Genesys.com. If Customer issues an instruction under this DPS, Genesys will document it for the duration of the DPS to ensure the accountability principle of the applicable Privacy Legislation.
   d. ***Data Ownership.*** Customer retains all rights, title and interest to its Customer Data. Customer grants Genesys a non-exclusive right to process, use, copy, store, transmit, modify, display, perform and create derivative works of Customer Data only to the amount as necessary to provide the Service as defined in the Master Agreement and as permitted by applicable law.
   e. ***Access or Use.*** Genesys will not access or use Customer Data except as necessary to provide the Service or as instructed by Customer.
   f. ***Disclosure.*** Genesys will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Genesys a demand for Customer Data, Genesys will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Genesys may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Genesys will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Genesys is legally prohibited from doing so.
   g. ***Genesys Personnel.*** Genesys personnel may not process Customer Data without proper internal authorization. All Genesys personnel receive data security and privacy training on an annual basis and have agreed to appropriate confidentiality obligations (for the term of their employment and thereafter), insofar as they are not already bound to do so in accordance with relevant legislations and regulations.

h. ***Data Controls.*** Insofar as a Data Subject contacts Genesys directly concerning a rectification, erasure, or restriction of processing, Genesys will forward the Data Subject's request as soon as reasonably possible to the Customer. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by Genesys without unreasonable delay, or Genesys will provide tools for Customer to fulfil such requests via the Service.

i. ***Transfers of Customer Data.*** Customer understands that the services provided by Genesys sometimes require Customer Data to be transferred to a country or territory outside the EEA. Customer agrees to Genesys performing any such transfer of Customer Data to any such country and to store and process the Customer Data in order to provide the Services. The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the applicable Privacy Legislation). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply if Genesys is acting as a sub-processor (as defined in the Standard Contractual Clauses) with respect to Customer Data, or once Genesys has adopted Binding Corporate Rules or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the applicable Privacy Legislation) outside the EEA.

j. ***Deletion and Return of Customer Data.*** After conclusion of the contracted work, or earlier upon request by the Customer, at the latest upon termination of the Master Agreement, Genesys shall make all documents, processing and utilization results, and data sets related to the Customer that have come into its possession available, in a data-protection compliant manner. Otherwise, such data will be subject to Genesys' data deletion policies. Any Services performed after the termination of the Master Agreement will require additional fees.

3. **RESPONSIBILITIES OF GENESYS**

a. ***DPO.*** Genesys has appointed a Data Protection Officer in accordance with the applicable Privacy Legislation. Genesys has appointed Mr Shahzad Muhammad Naveed AHMAD, VP Cloud Competence Center & Data Privacy EMEA, office phone +44 (0)1753418818, mobile: +447717861224, email address: Shahzad.Ahmad@Genesys.com as Data Protection Officer. The Customer shall be informed as soon as possible of any change of Data Protection Officer.

b. ***Security.***

i. *Security Procedures.* Genesys shall establish security procedures in accordance with applicable Privacy Legislation. The measures to be taken are appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. Genesys has taken into account the state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons. Please refer to Appendices for details.

ii. *Technical and Organizational Measures.* Genesys has implemented measures to maintain the security of its facilities and networks as set forth in the Appendices. The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for Genesys to implement alternative adequate measures, provided such changes do not reduce the security provided. Substantial changes will be documented.

iii. *Review of Genesys Security.* Customer is solely responsible for reviewing the information made available by Genesys relating to data security and making an independent determination as to whether the Services meet Customer's requirements and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.

4. **AUDITS**

a. ***Audits.*** At least annually, Genesys uses external auditors to vet its security measures. This audit will be performed by an independent third party who will produce an audit report ("**Report**"). The Report will be Genesys Confidential Information. Reports will be made available to Customer subject to a mutually agreed upon non-disclosure agreement ("**NDA**"). At Customer's written request, Genesys will provide Customer with a Report so that Customer can reasonably verify Genesys' compliance with the security obligations under this DPS. If the Standard Contractual Clauses apply, then Customer agrees to exercise its audit right by instructing Genesys to execute the audit as described in this Section. If Customer has not opted out of the Standard Contractual Clauses and desires to change this instruction regarding exercising this audit right, then Customer has the right to change this instruction, as mentioned in the Standard Contractual Clauses,

which shall be requested in writing. If the Standard Contractual Clauses apply, then nothing in this Section of the DPS varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

5. **SECURITY BREACH NOTIFICATION**
   a. ***Notification.*** Genesys will assist the Customer in complying with the reporting requirements for data breaches. These include:
      i. The obligation to report a personal data breach as soon as reasonably possible to the Customer. The parties are aware that data protection requirements impose a duty to inform in any event of the loss or unlawful disclosure of personal data or access to it. Such incidents should therefore be communicated as soon as reasonably possible to the Customer. Genesys will take appropriate measures to secure the data and limit any possible detrimental effect on the data subjects. Where Customer is obligated under applicable law to notify a government authority, Genesys is obliged to assist the Customer in preparing such notification.
      ii. The duty to assist the Customer to provide information to the Data Subject concerned, if required by the applicable Privacy Legislation, and to provide the Customer with all relevant information in this regard as soon as reasonably possible.

6. **SUBCONTRACTING**
   a. ***Subcontractors.*** Genesys may transfer data to its Affiliates and hire other companies to provide limited services on its behalf, such as assisting customer support. Any such Affiliates and subcontractors will be permitted to obtain Customer Data only to deliver the services Genesys has retained them to provide, and they are prohibited from using Customer Data for any other purpose. Genesys shall make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Customer's data, even in the case of outsourced ancillary services.
   b. ***Current Subcontractors.*** PureCloud resides within third party data centers provided by Amazon Web Services (AWS). In addition, our PureCloud offering uses third party vendors for monitoring, alerting and log storage. All syslog, app log, cloud trail and VPC flow details are sent to SumoLogic. Alert Logic and Threatstack are used for security monitoring, and New Relic is used for instance and application monitoring. New Relic. OneLogin is used for authentication, authorization and accounting. For Customer account info, its representatives contact details & Customer care tickets; Salesforce (SFDC) solution is used. Zuora solution is used for quoting and billing purpose. In addition, the following providers are used for PureCloud Voice PSTN connectivity: Verizon, Bandwidth.com, iBasis, Voxbone, Intrado and Brightlink (only relevant if customer is purchasing Voice PSTN connectivity).

Subprocessor	Address/country/website	Service
Amazon	Ireland or Germany AWS Region (www.amazon.com)	PureCloud build on AWS MicroServices
Sumo logic	https://www.sumologic.com	Log collection tool
Alert Logic	https://www.alertlogic.com/	Security/monitoring
Threatstack	https://www.threatstack.com	Security/monitoring
New Relic	https://newrelic.com	Security/monitoring
Onelogin	https://www.onelogin.com	authentication
Salesforce (SFDC)	https://www.salesforce.com	Account info and ticketing system
Zuro	https://www.zuora.com	Quoting & billing

   c. ***Changes to Subcontractors.*** Genesys shall inform Customer of any intended changes concerning the addition or replacement of subcontractors that has a material effect on the processing of Customer Data. If Customer has a reasonable basis to object to any such changes, Customer must notify Genesys of his objection within 10 days after receipt of Genesys' notice of the intended changes. Following such objection, Genesys will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration of the Services to address Customer's concerns. Should Customer persist in its objection, it may, as its sole and exclusive

remedy, terminate the Master Agreement under the condition that it pays all fees and charges for the remainder of the term of the Master Agreement.

7. **NONDISCLOSURE**
    a. ***Confidential Information.*** Customer agrees that the contents of this DPS are Confidential Information.

8. **ENTIRE AGREEMENT; CONFLICT**
    a. ***Entire Agreement; Conflict.*** Except as amended by this DPS, the Master Agreement will remain in full force and effect. If there is a conflict between the Master Agreement and this DPS, the terms of this DPS will control.

Attachments:

- DPS Attachment 1: Standard Contractual Clauses (SCC)
- DPS Appendix 1: Data and Processing Description
- DPS Appendix 2: Genesys Security Measures

DPS Attachment 1 **–Standard Contractual Clauses (SCC)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: *[ENTER CUSTOMER BUSINESS]*
Address: *[ENTER ADRESS OF Customer BUSINESS]*
Tel.: _____; fax: _____; e-mail: _____
Other information needed to identify the organisation:
……
(the data **exporter**)

and

Name of the data importing organisation: Genesys Telecommunications Laboratories B.V.
Address: Gooimeer 6-02, 1411DD Naarden, Netherlands
Tel.: +31 35 625 7230; fax: +31 35 678 2022; e-mail: legal@genesys.com , DataPrivacy@genesys.com
……
(the data **importer**)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in DPS Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in DPS Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in DPS Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of DPS Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in DPS Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of DPS Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……

(stamp of organisation)

DPS Appendix 1 to the Standard Contractual Clauses
Data and Processing Description

1. **Data exporter:** Customer is the data exporter.
2. **Data importer:** The data importer is Genesys.
3. **Data subjects**: Data subjects include the data exporter's customer's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer.
4. **Categories of data**: The personal data transferred includes names, titles, email, postal address, phone numbers, geo-locations, end-customer history, end-customer billing and invoicing data, and other data in an electronic form collected via the Services.
5. **Processing operations**: The personal data transferred will be subject to the following basic processing activities:
    a. ***Duration and Object of Data Processing***. The duration of data processing shall be for the term customized by the Customer. The objective of the data processing is the performance of Services.
    b. ***Scope and Purpose of Data Processing***. The scope and purpose of processing personal data is described in the Master Agreement. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities.
6. **Subcontractors**: The data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

DPS Appendix 2 to the Standard Contractual Clauses
Genesys Security Measures

This Appendix describes the minimum-security requirements applicable to Processors' provision to Customer. Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor as his role as processor for Customer shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Therefore, Processor will use necessary reasonable technical, organizational and security measures designed to protect personal Data of Customer in possession of Processor or otherwise processed by Processor against unauthorized access, alteration, disclosure or destruction, as further described in this Appendix:

1. **Security Program**
   We have implemented and will maintain an information security program that follows generally accepted system security principles embodied in the ISO 27001 standard designed to protect the Customer Data as appropriate to the nature and scope of the Services provided. PureCloud's Security & Compliance Team maintaining the information security program includes experienced professionals holding a wide range of certifications in both security and privacy. The information security program includes at least the following elements:

   a. **Security Awareness and Training**

      We have implemented and maintain an information security and awareness program that is delivered to employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass. Additionally, development staff members are provided with secure code development training.

   b. **Policies and Procedures**

      We maintain policies and procedures to support the information security program. Policies and procedures are reviewed annually and updated as necessary.

   c. **Change Management**

      We utilize a change management process based on industry standards to ensure that all changes to the PureCloud production environment are appropriately reviewed, tested, and approved.

   d. **Patching**

      PureCloud does not patch. The strategy is to destroy and rebuild all server instances at least every 30 days on new "gold images" that have current patch levels. Gold images are updated at least every two weeks with up-to-date security patches.

   e. **Data Storage and Backup**

      We create backups of critical Customer Data according to documented backup procedures. Backup data will not be stored on portable media. Customer Data stored on backup media will be encrypted using server-side encryption as provided by Amazon Web Services ("AWS").

   f. **Vulnerability Scanning and Penetration Testing**

      We conduct internal vulnerability scanning on a regular basis with automated scans and notifications. The scan results are analyzed to confirm identified vulnerabilities, and remediation is scheduled within a timeframe commensurate with the relative risk.

      On at least an annual basis, we conduct a vulnerability assessment and penetration testing engagement with an independent qualified vendor. Issues identified during the engagement are appropriately addressed within a reasonable time frame commensurate with the identified risk level of the issue. An executive summary or full test results reports can be made available to customer upon written request and will be subject to non-disclosure and confidentiality agreements.

g. **Malware Prevention**

Applications running within PureCloud were developed and are maintained utilizing industry standard secure coding practices, including peer coding review, security and unit testing, and adherence to secure coding techniques. We use industry standard practices to avoid the inclusion of any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan Horses) in applications running within PureCloud.

2. **Network Security**

AWS provides a strong foundation of security and compliance which we supplement by employing industry standard network security controls designed to protect Customer Data, including, but not limited to, the following:

a. **Intrusion Detection Systems**: We have implemented and maintain a host-based intrusion detection system and network-based instruction detection system designed to alert us in the event of suspicious activity.

b. **Data Connections:** We use HTTPS/TLS with AES-256 encryption to secure connections between browsers, mobile apps, and other components to PureCloud.

c. **Data Connections between PureCloud and Third Parties**: Transmission or exchange of Customer Data with you and any third parties authorized by you to receive the Customer Data will be conducted using secure methods (e.g., TLS, HTTPS, SFTP).

d. **Encrypted Recordings**: We encrypt call recordings by default. PureCloud generates customer specific encryption keys used to secure call recordings. Chat sessions are encrypted in transit.

e. **Encryption Protection**: We use industry standard methods to support encryption. We use a minimum of RSA 2048 bits for asymmetric key encryption. For symmetric key encryption, we use AES 128 bits. For hashing, we use SHA1 and SHA2.

3. **User Access Control**

We have implemented and maintain appropriate access controls and the concept of least privilege designed to ensure only authorized users have access to Customer Data within PureCloud. User access is logged for audit purposes.

a. **Customer User Access**

Customers are responsible for managing user access controls within the application. Customer defines the usernames, roles, and password characteristics (length, complexity, and expiration timeframe) for their users. Customer is entirely responsible for any failure by customer, agents, contractors or employees (including without limitation all of customer's users) to maintain the security of all usernames, passwords and other account information under customer control. Except in the event of a security lapse caused by our gross negligence or wilful action or inaction, customer is entirely responsible for all use of PureCloud through customer's usernames and passwords whether or not authorized by you and all charges resulting from such use. You will immediately notify us if you become aware of any unauthorized use of the PureCloud production environment.

b. **Our User Access**

We will create individual user accounts for each of our employees or contractors that have a business need to access the PureCloud production environment. The following guidelines will be followed with regard to our user account management:

i. User accounts are requested and authorized by our management.

ii. User accounts follow the concept of least privilege.

iii. Access to the PureCloud Production environment requires multifactor authentication.

iv. SSH keys are utilized instead of passwords within PureCloud.

v. Dormant or unused accounts are disabled after 90 days of non-use.

vi. Session time-outs are systematically enforced.

vii. User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

4. **Business Continuity and Disaster Recovery**

PureCloud is deployed and configured in a redundant infrastructure through AWS. Services provided by PureCloud follow a stateless architecture. Data repositories in PureCloud use redundancy and replication designed to maintain availability and avoid data loss in the event of a lost data node. The PureCloud environment is physically separated from our corporate network environment so that a disruption event involving the corporate environment does not impact the availability of the PureCloud Services.

a. **Business Continuity**

We will maintain a corporate business continuity plan designed to ensure that ongoing monitoring and support services will continue in the event of a disruption event involving the corporate environment.

b. **High Availability**

PureCloud utilizes AWS services to provide highly available environments, including, but not limited to, the following:

i. Availability Zones (AZs) which consist of one or more discrete data centers, each with redundant power, networking and connectivity, and housed in separate facilities;

ii. Auto Scaling Groups (ASGs) to dynamically scale clusters based on demand and automatically launch replacement instances in the event of a failure.

iii. AWS Elastic Load Balancers (ELBs) to route internal and external traffic to healthy infrastructure and automatically reroute traffic away from unhealthy infrastructure;

iv. Durable message queueing systems that support request queuing and point-to-multipoint notifications. Message queues allow us to both load-balance requests/events and handle load bursts without data loss; and

v. Amazon Simple Storage Service (S3). S3 stores objects redundantly on multiple devices across multiple facilities in an Amazon S3 Region. Amazon aims to deliver eleven 9's of durability.

5. **Security Incident Response**

We maintain a Security Incident response program based on industry standards designed to identify and respond to suspected and actual Security Incidents involving Customer Data. The program will be reviewed, tested and, if necessary, updated on at least an annual basis. "Security Incident" means a confirmed event resulting in the unauthorized use, deletion, modification, disclosure, or access to Customer Data.

a. **Notifications**

In the event of a confirmed Security Incident involving the unauthorized release or disclosure of Customer Data or other security event requiring notification under applicable law, we will notify customers within thirty six (36) hours and will reasonably cooperate so that customer can make any required notifications in connection with such event, unless we are specifically requested by law enforcement or a court order not to do so.

b. **Notification Details**

We will provide the following details regarding the confirmed Security Incident to customer: (i) date that the Security Incident was identified and confirmed; (ii) the nature and impact of the Security Incident; (iii) actions already taken by us; (iv) corrective measures to be taken; and (v) evaluation of alternatives and next steps.

c. **Ongoing Communications**

We will continue providing appropriate status reports to customers regarding the resolution of the Security Incident, continually work in good faith to correct the Security Incident and to prevent future such Security Incidents. We will cooperate, as reasonably requested by you, in order to further investigate and resolve the Security Incident.

6. **Privacy**

We have developed and will maintain a privacy program designed to respect and protect Customer Data under our control, and this is located at https://help.mypurecloud.com/articles/purecloud-privacy-policy/. We will not rent, sell or otherwise share any Customer Data with outside parties. Customer Data will only be used or accessed for the purpose of providing PureCloud Services.