END USER AGREEMENT
PURECONNECT

*****CONFIDENTIAL*****

This End User Agreement **("EUA")**, effective on the date of last signature **("Effective Date")** is made between the Licensor and the **"Customer"** being the entities named on the signature block below Capitalized terms shall have the meanings defined in the EUA.

1. SERVICES

1.1. Subject to the terms of the EUA, Customer is granted a non-transferable, non-sublicensable, non-exclusive Subscription to access and use the Genesys Cloud Service during the Subscription Term.

1.2. Licensor will provide Support as described in the Genesys PureConnect Cloud Services Support Policy, attached to this EUA as Exhibit A.

2. TERM AND TERMINATION

2.1. The term of the EUA shall commence upon the Effective Date and shall continue for the duration of any effective Services Orders. The Initial Subscription Term will commence upon the Scheduled Provisioning Date.

2.2. In the absence of a written non-renewal notice provided at least sixty (60) days prior to the end of the applicable Term, each Subscription Term shall automatically renew for Renewal Subscription Terms as set forth in the applicable Services Order.

2.3. Either party will have the right to terminate the EUA by written notice to the other party if (a) the other party has breached a material obligation under the EUA or any Services Order or SOW and such breach remains uncured for a period of thirty (30) days after written notice of such breach is sent to the other party; provided such breach is curable, it being understood that a breach of Sections 3.1 and 3.2 are incurable.; or (b) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

2.4. Notwithstanding any term in the EUA to the contrary, Genesys reserves the right to suspend the Genesys Cloud Services, or portion thereof, or reject or cancel the transmission of any information through the Genesys Cloud Service based upon (i) reasonable belief that the use of the Genesys Cloud Services is in violation of applicable Laws, (ii) Customer's 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, Genesys will provide notice of the suspension and keep Customer reasonably informed of Genesys' efforts to restore the Genesys Cloud Services.

3. INTELLECTUAL PROPERTY

3.1. All Intellectual Property Rights in the Services (and other materials or services provided hereunder) remain the exclusive property of Genesys and its licensors or suppliers, as applicable. Genesys and its licensors and suppliers reserve all rights not expressly granted in this EUA and own all rights in all Derivative Works of the Services (and other materials provided hereunder) and any copy, translation, modification, adaptation or derivation (including any improvement or development) of the Services (and all other materials provided hereunder).

3.2. No implied licenses are granted hereunder. Customer is granted no rights in or to the Services except as expressly set forth in this EUA and under a Services Order. Customer shall not (a) modify or create any Derivative Works, functionally equivalent works, or translations of the Services or any other materials provided hereunder, (b) reverse engineer the Services or take any action that jeopardizes Genesys' rights or the rights of its licensors and service providers in any materials, including the Services, made available to Customer hereunder; (c) access the Services in order to build a competitive product or service or to assist anyone else to compete with Genesys; or (d) use the Services in a way that violates any Law. Genesys Cloud Services include tools that can be used to create content related to Customer Data. The algorithms, compilations, collation methods and anonymized analyses created through the use of Genesys Cloud Services are considered Derivative Works and therefore are retained by Genesys. Customer retains, however, non-anonymized analyses of Customer Data obtained from

its use of such tools.

3.3. As between the parties, the Customer Data are the proprietary material of Customer and shall be considered Customer's Confidential Information. Customer grants to Licensor and Genesys a non-exclusive, non-sublicenseable (except to parties working on Genesys' behalf), non-transferable, royalty-free license to access, process, store, transmit, and otherwise make use of the Customer Data as directed by Customer or as necessary to provide the Services and to otherwise fulfill its obligations under and in accordance with the EUA.

3.4. To the extent not already owned by Genesys or Licensor and subject in each case to Section 11.1 to the extent Customer is identified by name or logo, Customer, on behalf of itself and its Related Parties, hereby grants Genesys and Licensor 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.

3.5. Nothing in this EUA precludes or limits Licensor or Genesys in any way from providing materials or services that are similar to materials or services provided or contemplated in this EUA 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 EUA, regardless of their similarity to any Services. Genesys and Licensor will be free to use any concepts, processes, techniques, improvements or other know-how developed by Genesys or Licensor in the course of performance of this EUA free from any use restriction or payment obligation. For the avoidance of doubt, but subject to this EUA, including this Section 3.5, neither Genesys nor Licensor claim any rights to any of Customer's Confidential Information.

4. WARRANTIES

4.1 Licensors warrants that the Maintenance and Support will be performed in a professional and workmanlike manner and in accordance with applicable requirements of this EUA.

4.2 Licensor warrants that the Genesys Cloud Services will materially conform to the specifications set forth in the Documentation. For purposes of this Section 4, "Documentation" shall mean applicable technical published manuals that accompany the Genesys Cloud Services.

4.3 Customer's sole and exclusive remedy for breach of the warranties set forth in this section shall be for Licensor to re-perform non-conforming services or to correct errors.

4.4 EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 4, THE SERVICES ARE PROVIDED TO CUSTOMER ON AN "AS IS" 'WHERE IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTY OF ANY KIND EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. GENESYS MAKES NO REPRESENTATIONS OR WARRANTIES THAT USE OF THE GENESYS CLOUD SERVICE WILL BE UNINTERRUPTED, TIMELY, COMPLETE, OR ERROR-FREE.

5. LIMITATION OF LIABILITY

5.1. THE CUMULATIVE AGGREGATE LIABILITY OF A PARTY AND ALL OF ITS RELATED PARTIES (AND IN THE CASE OF LICENSOR, ITS LICENSORS OR SERVICE PROVIDERS) UNDER THE EUA SHALL BE LIMITED TO DIRECT DAMAGES AND SHALL NOT EXCEED THE FEES PAID TO LISENSOR DURING THE TWELVE MONTHS IMMEDIATELY PRIOR TO THE COMMENCEMENT OF THE DISPUTE FOR THE SERVICES THAT ARE THE SUBJECT OF THE DISPUTE. CUSTOMER AGREES THAT THIS LIMITATION ON LIABILITY FORMS A FUNDAMENTAL BASIS OF THE BARGAIN HEREUNDER, IN THE ABSENCE OF WHICH, THE ECONOMIC TERMS OF THIS EUA WOULD HAVE BEEN DIFFERENT.

5.2. IN NO EVENT SHALL EITHER PARTY OR ANY OF ITS RELATED PARTIES (AND IN THE CASE OF LICENSOR, ITS LICENSORS OR SERVICE PROVIDERS) BE LIABLE TO THE OTHER PARTY OR ANY OF ITS RELATED PARTIES (AND IN THE CASE OF LICENSOR, ITS LICENSORS OR SERVICE PROVIDERS) FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE DAMAGES OF ANY CHARACTER, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING LOSS OF BUSINESS OR GOOD WILL, WORK STOPPAGE, LOST

PROFITS, REVENUE, DATA OR USE, COMPUTER FAILURE OR MALFUNCTION AND TELECOMMUNICATIONS CHARGES FROM UNAUTHORIZED ACCESS), COVER DAMAGES , OR OTHER SIMILAR DAMAGES REGARDLESS OF THE LEGAL THEORY ASSERTED, WHETHER IN CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, STRICT LIABILITY OR OTHERWISE, EVEN IF SUCH PARTY OR ANY OF ITS RELATED PARTIES (AND IN THE CASE OF LICENSOR, ITS LICENSORS OR SERVICE PROVIDERS) HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF AN AGREED REMEDY FAILS OF ITS ESSENTIAL PURPOSE OR IS HELD UNENFORCEABLE FOR ANY OTHER REASON.

5.3. THIS LIMITATION OF LIABILITY SHALL NOT OPERATE SO AS TO: (I) REDUCE ANY AMOUNTS DUE AS FEES; (II) LIMIT LIABILITY ARISING IN CONNECTION WITH INDEMNIFICATION OBLIGATIONS; OR (III) LIMIT LIABILITY FINALLY DETERMINED TO HAVE RESULTED FROM A PARTY'S GROSS NEGLIGENCE OR WILFULL MISCONDUCT. 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).

6. CONFIDENTIALITY

6.1. During the Confidentiality Period, recipient shall (a) protect the confidentiality of all Confidential Information using the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but in no event less than reasonable care) to prevent unauthorized use or disclosure; (b) not use any Confidential Information except as expressly authorized in the EUA; (c) not disclose, orally or in writing, any Confidential Information to any person, other than an employee, consultant or agent of recipient bound by terms at least as restrictive as those set forth herein with a need to know such Confidential Information.

6.2. The obligations in Section 6.1, however, shall not apply to any information which: (a) is already in the public domain or becomes available to the public through no breach of the EUA by recipient; (b) was in the recipient's possession prior to receipt from discloser, as proven by recipient's written records; (c) is received by the recipient from a third party free to disclose such information to recipient; or (d) is independently developed by recipient without use of the Confidential Information.

6.3. Nothing in this EUA shall prevent a party from disclosing Confidential Information to the extent required by applicable Law, judicial or administrative process, provided that recipient shall: (i) notify discloser of any duty to disclose, affording opportunity for discloser to take protective actions (except to the extent notice is prohibited by Law), and (ii) disclose only as much of the Confidential Information as required, maintaining all proprietary notices applicable to such Confidential Information.

6.4. Upon written request in connection with termination of the EUA, each party shall deliver to the other party or destroy all copies of such other party's Confidential Information. Notwithstanding the foregoing, recipient may retain an archival record of Confidential Information to the extent required pursuant to applicable Law subject to recipient's compliance with the remaining terms of this section.

7. COMPLIANCE WITH LAWS

Each party shall comply with all applicable Laws in connection with the performance of its obligations under this EUA. Notwithstanding the foregoing, however, Licensor is not responsible for ensuring that the Services, or Customer's use thereof, comply with any Laws applicable to Customer's business or industry, including, without limitation communications and privacy regulations such as the Telephone Consumer Protection Act of 1991 and the Health Insurance Portability and Accountability Act (HIPAA).

8. USE OF THE SERVICE

8.1. Customer will not, and will not permit or authorize others, to use the Genesys Cloud Service for any of the following:

8.1.1. to violate applicable Law;

8.1.2. to transmit Malicious Code;

8.1.3. to transmit 911 or any emergency services (or reconfigure to support or provide such use);

8.1.4. to interfere with, unreasonably burden, or disrupt the integrity or performance of the Genesys Cloud Services or third-party data contained therein;

8.1.5. to attempt to gain unauthorized access to systems or networks; or

8.1.6. to provide the Genesy s Cloud Services to non-User third parties, including, by resale, license, lend or lease.

8.2. Customer will use commercially reasonable efforts to prevent and/or block any prohibited use by Customer personnel or Customer's Users.

8.3. Customer will maintain any reasonable, appropriate administrative, physical, and technical level of security regarding its account ID, password, antivirus and firewall protections, and connectivity with the Genesys Cloud Services.

8.4. Customer shall maintain strict security over all VoIP Services lines. Customer acknowledges that Genesys does not provide Customer the ability to reach 911 or other emergency services and Customer agrees to inform any individuals who may be present where the Genesys Cloud Services are used, or who use the Genesys Cloud Services, of the non-availability of 911 or other emergency dialing.

8.5. If the Genesys Cloud Service will be used to transmit or process Sensitive Information, Customer will ensure that all Sensitive Information is captured and used solely via the use of available Security Features.

8.6. Recordings. As between the parties, Customer acknowledges that Recordings are solely within its discretion and control. Without limiting the foregoing: (i) Customer accepts sole responsibility for determining the method and manner of performing Recording such that it is compliant with all applicable Laws and for instructing the Services accordingly; and (ii) Customer shall ensure that Recordings shall be made only for diagnostic, quality assurance, archival, and/or Support purposes, and in any event only for purposes required and/or in compliance with, all applicable Laws. Customer will ensure that either (a) Recordings will not knowingly include any bank account number, credit card number, authentication code, Social Security number, or other personal or Sensitive Information, except as allowed or required by all applicable Laws; or (v) Recordings are encrypted at all times. To the extent Recordings are encrypted or where encryption is electable by Customer as part of the Service, Customer shall elect such encryption. Customer shall not modify, disable, or circumvent the Recording encryption feature within the Genesys Cloud Services and shall otherwise ensure that it will use the Genesys Cloud Services in compliance with the encryption feature.

9. CUSTOMER DATA

9.1. General.

9.1.1. Customer acknowledges and agrees that the Customer Data may be transferred or stored outside the country where Customer and its customers are located in order to carry out the Services and Genesys' other obligations under the EUA.

9.1.2. Customer represents and warrants that it has obtained all consents necessary for Licensor, its suppliers, licensors (including Genesys), and partners to collect, access, process, store, transmit, and otherwise use Customer Data in accordance with the EUA.

9.1.3. Customer shall comply with all requirements of integrity, quality, legality and all other similar aspects in respect of Customer Data and Messages. Licensor, its suppliers, licensors (including Genesys), and partners may, but are not obligated to, review or monitor any Customer Data. Licensor, its suppliers, licensors (including Genesys), and partners expressly disclaims any duty to review or determine the legality, accuracy or completeness of Customer Data used through the Genesys Cloud Services.

9.1.4. If Customer, End Users or Persons provide credit card information to the Genesys Cloud Services, Customer retains responsibility for compliance with all applicable standards, including the Payment Card Industry Data Security Standards ("PCI-DSS"). The Genesys PureConnect Cloud Service is PCI compliant, provided that Customer purchases the Premium Services described in Exhibit B, Section 10. Customer agrees to not send PCI data without purchasing the applicable Premium Services.

9.2. Protection of Customer Data.

9.2.1. Unless Customer's failure to comply with Section 8 prevents Licensor and Genesys from doing so, Genesys shall maintain reasonable, appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data.

9.2.2. Neither Licensor nor Genesys will modify, disclose, or access Customer Data except to provide the Services and perform Support to prevent or address service issues or technical problems, at Customer's request in connection with Support, or to the extent otherwise permitted in the EUA.

10. INDEMNIFICATION

10.1. Subject to the Exclusions, Genesys shall, at Genesys's expense, pay to defend Customer and indemnify Customer against any judgments finally awarded by a court and pay any settlements approved by Licensor with respect to any non-affiliated third-party claims that the original, unchanged Genesys Cloud Service, as it stands alone, infringes or misappropriates any third party's Intellectual Property Rights as identified in a patent or copyright that is valid and enforceable in the United States. Genesys may at any time and at its option and expense: (i) obtain for Customer the right to continue using the Genesys Cloud Service, (ii) modify or replace the Genesys Cloud Service so that it becomes non-infringing while retaining substantially similar functionality; or (iii) if neither of the foregoing remedies can be reasonably effected, terminate Customer's right to use the Genesys Cloud Service and refund any prepaid, unused Fees. The provisions of this Section 10 state the sole, exclusive, and entire liability of Genesys and are Customer's sole remedy with respect to the infringement of third party intellectual property rights.

10.2. Customer, at Customer's expense, will defend and indemnify Genesys and its Related Parties against any judgments finally awarded by a court, and pay any settlements approved by Customer with respect to any claims: (a) that Customer Data and/or Customer's method or process of doing or conducting business infringes any Intellectual Property Rights of a third party; (b) arising from Customer's non-compliance with Section 3 (Intellectual Property); or (c) that the Genesys Services or the use thereof infringes any Intellectual Property Rights of a third party to the extent such claim arises in connection with an Exclusion(s).

10.3. A party entitled to indemnification ("Indemnified Party") shall take all reasonable steps to mitigate any potential expenses and shall work with the Licensor to provide the other party (the "Indemnifying Party") with: (i) prompt written notice of any such claim or actions, or possibility thereof upon becoming aware of the same; and (ii) relevant information (subject to confidentiality restrictions the Indemnified party owes to third parties), authority, and reasonable assistance to settle or defend and such claim or action. 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 Indemnified Party shall tender sole control and authority over to the Indemnifying Party and reasonably assist with the defense or settlement of such claim or action. Notwithstanding the foregoing, the Indemnified Party shall have the right to retain counsel of its own choice, at its own expense, in respect of the subject of the Indemnification, for purposes including services as co-counsel, or to monitor the defense provided by the Indemnifying Party's appointed counsel. The Indemnified Party shall have the right to approve counsel selected by the Indemnifying Party, which approval shall not be unreasonably withheld or delayed.

11. MISCELLANEOUS

11.1. Marketing. Subject to Customer's written consent in each instance, Customer grants Licensor and Genesys the right to use Customer's name and logo to identify Customer as a Genesys customer. Subject to prior written approval of content, Customer grants Licensor and Genesys the right to issue a media release after execution of the EUA announcing that Customer has become a Genesys customer, and to make other announcements and place promotion in various publications and media. Customer agrees that, not less than once per calendar quarter during the Term of this EUA, to act as a reference customer as requested by Genesys. Except as set forth in a mutually agreed written public statement, Customer will not imply or state that Customer is affiliated with or endorsed by Genesys, publicize the existence of the EUA, or disclose any of its terms.

11.2. Assignment. Neither party may assign its rights or obligations under the EUA, 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, or (2) with the

prior written consent of the other party, which shall not be unreasonably withheld. 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.

11.3. Government Usage. This is a commercial item EUA. If the Services are acquired by or on behalf of the U.S. Government, a state or local government, or a prime contractor or subcontractor (of any tier) of the foregoing, such government customers and users shall obtain only those commercial license rights set forth in the EUA.

11.4. Survival: The provisions of the EUA regarding payment, confidentiality, assignment, licenses, definitions, limitation of liability, intellectual property and any provision which by its nature should survive, will survive the termination of the EUA. In the event that any provision of the EUA is held to be invalid or unenforceable, the remaining provisions of the EUA shall remain in full force.

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

11.6. Governing Law: This EUA shall be governed by the laws set forth in Table 1 below, based on the Customer's domicile, without reference to conflicts of law provisions. The parties agree to submit to the personal and exclusive jurisdiction of such courts and that venue therein is proper and convenient as set forth in Table 1. In the event more than one entity is or becomes a party the EUA, the governing law shall be California and United States federal law; and, the California state courts in and for San Mateo County, California (or, if there is federal jurisdiction), the United States District Court for the Northern District of California, each of which shall have the personal and exclusive jurisdiction, which such jurisdiction is acknowledged to be proper and convenient. The UN Convention for the International Sale of Goods shall not apply to the EUA in whole or in part. In any dispute under the EUA, the prevailing party shall be entitled to recover its cost of enforcing its claim, including but not limited to attorney fees.

11.7. Authority to Execute: The party executing the EUA on behalf of the parties represents and warrants that he or she has been duly authorized under the party's charter documents and applicable law to do so.

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

11.9. Third party beneficiaries: Both parties acknowledge that Genesys and Genesys Telecom Inc are intended third-party beneficiaries of this EUA and that no other third-party beneficiary relationships are created by this EUA.

11.10. Notices: All notices under the EUA shall be in writing and shall be deemed to have been given when (a) personally delivered; (b) sent by electronic facsimile transmission; or (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) or (d) 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). Notices to either party shall be sent to the applicable address set forth in the preamble of the EUA or such other address as a party may notify the other party of in writing.

11.11. Waiver: No provision of the EUA may be waived unless such waiver is in writing and signed by the party against which the waiver is to be effective.

11.12. Complete EUA; **Amendmen**t. The EUA constitutes the complete EUA between the parties and supersedes all prior EUAs and representations, written or oral, concerning the subject matter of the EUA. In the event of a conflict between the terms of a Services Order and the other provisions of the EUA, the terms of the Services Order shall take precedence; however, , Sections 5 (Limitation of Liability), 7 (Compliance with Laws), 8 (Use of Service), 9 (Customer Data) and this section 11.12 (Complete Agreement) of the EUA may only be modified in the Services Order by a direct reference to such sections. The EUA may not otherwise be modified or amended except in a writing signed by a duly authorized representative of each party. The terms of the EUA shall supersede the terms in any Customer purchase order or other ordering document.

11.13. Execution; Digitized Copies. The parties agree that this EUA may be executed by any means of signature, including electronic commerce or transmission, including facsimile, email, or acknowledgement through a webpage. The EUA 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 EUA and other associated documents, including attachments and amendments shall

legally bind the parties to the same extent as original documents.

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

12. DEFINITIONS

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.

Confidential Information: Any information disclosed by one party to the other party, or otherwise learned by the recipient from the discloser, marked "confidential" or disclosed or learned under circumstances that would lead a reasonable person to conclude that the information was confidential. Notwithstanding the foregoing, Genesys Confidential Information includes but is not limited to the Services and the terms of this EUA and Customer Confidential Information includes but is not limited to Customer Data. In addition, whether or not marked "confidential" or otherwise identifiable as confidential, the following information shall be deemed Confidential Information of the discloser: inventions, product development plans, education materials, pricing, marketing plans, and customer lists.

Confidentiality Period: The longer of: (i) three (3) years after termination of the EUA, or (ii) indefinitely with respect to trade secrets, Customer Data, and the Services.

Customer Data: (a) all data submitted through the Genesys Cloud Service by Customer or Users; and (b) the non-anonymized content of any reports generated by the Genesys Cloud Service regarding Customer's use of the Genesys Cloud Service.

Derivative Work: A new or modified work that is based on or derived from all or any part of the Services, including without limitation, a revision, modification, translation, localization, adaptation, abridgment, port, condensation or expansion, in any form, of the Services, or any work that would infringe any copyright if created without the authorization of the copyright holder or any other intellectual property right in the Services or that uses trade secrets or other Confidential Information embodied in or used by the Services.

Effective Date: The effective date of the EUA, which shall be the date both parties have signed the EUA.

Exclusions: are conditions that are deemed excluded from, and that terminate, Licensor's and/or Genesys's warranty, defense or indemnity obligations, as follows: (i) use of Genesys Cloud Service in combination with any non-Genesys equipment, software, services, processes, data or materials; (ii) Customer's non-compliance with this EUA or Documentation; (iii) use of the Genesys Cloud Service after receipt of notice from Genesys to discontinue such use; (iv) the development or use of any alteration, derivation, modification or customization of the Genesys Cloud Service regardless of whether developed by Genesys, Customer, or any other person or entity and regardless of whether developed using any Genesys tools, methods or training; (v) Genesys's compliance with Customer's requests or instructions or the use of any materials provided by Customer; (vi) Customer's business method(s) or process(es); (vii) Customer content or Customer Data.

Feedback: any suggestions, enhancement requests, recommendations, report, feedback, proposals, anonymized statistical data or other information concerning the Genesys Cloud Service provided by Customer to Genesys hereunder. 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.

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.

Genesys Cloud Service(s): The individual services and use of features and functionality of Genesys proprietary software and supporting facilities, all as further described in this EUA and the Documentation, that are ordered by Customer by a Services Order. The term "Genesys Cloud Service" excludes Professional Services, Support and the use of Third-Party Applications.

Indemnify (and all forms of the word (e. g. Indemnification): EUA to indemnify, hold harmless, and defend the other party and its Related Parties and from and against any and all non-affiliated third-party claims, demands, sums of money,

actions, rights, causes of action, obligations, allegations and liabilities of any kind or nature whatsoever, and from any resulting liabilities, damages, losses, and costs (including, but not limited to, attorney fees and disbursements) arising from or relating, directly or indirectly, to the use, act, omission, or manner set forth as the subject of and giving rise to the claim.

Initial Subscription Term: The minimum term for the initial Subscription under each Services Order.

Intellectual Property Rights: Any and all technology, know-how, software, data, ideas, formulae, processes, charts, Confidential Information, and any other materials or information and any and all worldwide intellectual property rights (present and future) therein and thereto, including copyrights, trade secrets, patents, patent applications, moral rights, contract rights and other proprietary rights.

Law(s): Laws, statutes, regulations, directives, rules, standards and the like of any territorial division (e. g. federal, national, state, province, etc.).

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.

Professional Services (or PS): The professional services described in a Statement of Work executed by the parties.

Recordings: Recorded inbound or outbound Genesys VoIP Service transmission, performed by Customer, via the Genesys Cloud Service.

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.

Renewal Term(s): Each subsequent term of a Services Order after the Initial Subscription Term.

Security Features: The features and functionality associated with the Genesys Cloud Service used to help secure transmitted data. Security Features may include secure SIP/RTP, voice connection encryption, log masking, or other similar features.

Sensitive Information: All sensitive Customer Data, including but not limited to personal health information (PHI), personally-identifiable information (PII) and credit card information.

Services: The Genesys Cloud Service, Support, and all related services provided under the EUA.

Service Level EUA: Genesys's agreement to perform the Genesys Cloud Services in accordance with specific metrics, subject to a defined set of remedies as set forth in Section 2 of Exhibit A to this EUA.

Services Order(s): The document by which Customer orders Genesys Cloud Services, or other goods and services that Customer may purchase from Genesys pursuant to this EUA. Services Order shall include: (a) a description of items being ordered, including Subscription Term, and the quantity, (b) Fees, method of determining Fees, and pricing terms, (c) billing address; and (d) other addresses for the parties, if applicable. Genesys reserves the right to waive any or all of the aforementioned requirements either in writing or by fulfilment of the Order.

Subscription: Term-based grant, for a specified time to use a specific quantity and type of Genesys Cloud Service, all as described in the applicable Services Order. Subscriptions exclude services and expenses associated with decommissioning Customer's use of the Genesys Cloud Service, migration of Customer Data, and storage and retrieval of records associated with Customer's use of the Services.

Subscription Term: The Initial Subscription Term and all Renewal Subscription Terms.

Support: the maintenance and support of the Genesys Cloud Service, subject to the terms and policies set forth in Exhibit A of this EUA.

Support Level: The applicable level of Support as selected by Customer and elected under the Services Order.

Taxes and Regulatory Fees: Any direct or indirect local, state, federal or foreign taxes, levies, duties or similar governmental assessments of any nature, including regulatory fees (such as USF), fines, penalties, value-added, use or withholding taxes. Taxes and Regulatory Fees shall not include charges based upon Genesys' income or employees.

Term: Any term (time period) under the EUA (e. g. Subscription Term, License Term).

Third-Party Applications: Third party or Customer-developed online, Web-based applications and offline software products that are provided by Customer or third parties, that may or may not interoperate with the Genesys Cloud Service.

[REMAINDER OF THE PAGE INTENTIONALLY LEFT BLANK]

Table 1. Governing Law, Jurisdiction, Notices.

If Customer, as of the Effective Date of the Service Order, is domiciled in:	The governing law is:	The courts have exclusive jurisdiction are:
Australia	The laws of the State of New South Wales, Australia govern this EUA. Each party irrevocably submits to the non-exclusive jurisdiction of the courts of New South Wales, Australia and waives any objection to proceedings in such courts on grounds of venue or that the proceedings have been brought in an inconvenient forum.	
Brazil	Brazil	The courts located in Sao Paulo, State of Sao Paulo, Brazil.
Canada	Ontario, and the applicable Canadian Federal law	The courts of Ontario, in the courts located in Toronto, Ontario
Japan	Japan	The courts of Japan, in the courts located in Tokyo, Japan

Korea	The Republic of Korea.	The courts of the Republic of Korea.
Singapore	The Republic of Singapore	The courts of the Republic of Singapore
United States	California, and the applicable United States federal law	The California state courts in and for San Mateo County, California or, (if there is Federal jurisdiction), the United States District Court for the Northern District of California
Rest of World/Other	England and Wales	The courts of England and Wales in the courts located in London, England

END USER AGREEMNT
SUPPLEMENTAL TERMS: PURECONNECT

*****CONFIDENTIAL*****

2. Equipment

Licensor may offer Equipment for resale or renting on a pass-through basis under limited circumstances under this EUA. All Equipment is provided "AS-IS" without warranty of any kind and is excluded from the scope of any warranty or indemnification obligations that may be provided under this EUA. In the event Customer rents Equipment, Customer shall pay such Fees as reflected in the Services Order. Customer shall secure and protect rented Equipment at Customer's location(s). In the event rented Equipment is lost, stolen or damaged, Customer agrees to reimburse Licensor for reasonable replacement costs. Upon termination of the Services Order, Customer will promptly return rented Equipment to Licensor in good condition, reasonable wear and tear excepted. Shipping terms are F.O.B. In the event Customer purchases Equipment from Licensor, Customer shall pay such Fees as reflected in the Services Order and title to such Equipment transfers to Customer upon full payment. Customer will retain purchased Equipment upon termination or expiration of the EUA. Any other equipment or facilities required by Customer to access the Genesys Cloud Services will be provided by and paid for by Customer.

3. Communication Circuits

Customer is responsible for procuring the applicable Communication Circuits for use with Genesys Cloud Services. If set forth in the Services Order, Customer may procure access to Communication Circuits from Licensor subject to payment of associated installation charges (one-time, per circuit), and access fees (monthly). Communication-related Fees include any fees or charges imposed by third party carriers or service providers to install or initiate service for Customer (e.g., Communications Circuits installation fees).

4. Inbound and Outbound Long Distance Services

Customer is responsible for procuring the applicable communication services, including inbound and outbound voice, data, long distance and external network facilities for use with Genesys PureCloud Services. If set forth in the Services Order, Licensor will administer Customer's access to domestic and international inbound and outbound long distance services from one or more telecommunication Providers in connection with Customer's use of the Cloud Services. Except as otherwise set forth in the Services Order, long distance services are billed separately each month based on Customer's usage, subject to a minimum access charges, plus applicable taxes.

5. Agent Training

Training is available subject to additional fees and expenses. As set forth in the applicable Services Order, Licensor will provide initial user training to Customer's trainer and administrative Agents. Classroom or in-person training shall be conducted at a mutually acceptable location and date. Customer will cause one or more of its employees to attend "Train the Trainer" training prior to the planned Provisioning Date. Thereafter, Customer's trainer will conduct user training for Customer's Agents that are expected to commence use of the Genesys Cloud Services as of the planned Provisioning Date. Following the planned Provisioning Date, Customer's trainer will provide user training on an ongoing basis to enable Customer's Agents continued use and understand the functionality of the Genesys Cloud Services as appropriate for the Agents' areas of responsibility.

6. Reports

Customer's use of the Genesys Cloud Service may include access to certain reporting tools. Customer personnel that have completed required training can configure reporting tools. Customer may use and distribute Reports for Customer's internal use only.

7. Workforce Optimization; Business Analytics

As set forth in the Services Order, the Subscription may include access and use of workforce optimization and business analytics software or tools, or adapters that integrate with third party workforce management tools

("WFO"). Customer is responsible for all decisions made using WFO and for determining whether WFO is sufficient for its needs. WFO Reports, including but not limited to forecasting, reflect estimates using certain categories of available historical data and generalized staffing or other projections which may not reflect or be otherwise suitable for Customer's specific needs.

8. Support

The PureConnect Service will be made available 24 hours a day, 7 days a week, except for: (a) occasional planned downtime at non-peak hours (for which advance notice will be provided); or (b) any unavailability causes by circumstances beyond Genesys's reasonable control, including failure or delay of Customer's internet connection, misconfiguration by Customer or any third party, issues on Customer's network, or telecommunications services contracted by or for Customer. The PureConnect Support Policy is attached here to as Exhibit A.

9. Data Security

Security and privacy policies for the Genesys PureConnect Service, which are incorporated by reference, are attached hereto as Exhibit B. Customer shall comply with all applicable security guidelines, which shall be in accordance with industry standards. Customer is solely responsible for the content and legal sufficiency of its Customer Data.

10. Transition Services

Transition services to facilitate migration of the services to a replacement provider, to archive or migrate Customer Data, or to otherwise wind-down the services ("Transition Services") are excluded from the scope of the Subscription. Licensor will make Transition Services available to Customer subject to the parties' execution of a separate statement of work. If Customer is in breach of the EUA as of the Subscription termination date, Licensor may condition its performance of Transition Services upon Customer's pre-payment in full for Transition Services and other outstanding amounts.

11. Definitions

As used in the applicable Services Order, SOW or these Supplemental Terms, capitalized terms shall have the meanings set forth below:

Agent: Customer's Users who answer and place calls via a call center.

Communications Circuits: Data and voice communications circuits provided by one or more telecommunications service Providers for use with Genesys Cloud Services.

Concurrent User: The peak number of simultaneous Users at a point in time.

Data Center: means a data center where we house servers and other components used to deliver the PureConnect Service.

Equipment: Non-Genesys, third party product provided on a pass-through basis without warranty from Genesys.

Full Production: The day upon which the earlier of the following occurs: (i) Customer reaches the agreed Minimum Monthly User/agent commitment counts as shown in the Services Order; (ii) Customer notifies Genesys of its intent to end the Ramp Period; or (iii) the Ramp Period expires.

Infrastructure Provisioning Fee: The Fee set forth in a Services Order due to be paid to Genesys by Customer in respect of the provisioning of the applicable Genesys infrastructure environment.

Live: The earlier of (a) the day in which there is at least one (1) User of the PureConnect Services in an environment capable of supporting the agreed Minimum Monthly User/agent commitment counts as shown in the Services Order, or (b) thirty (30) days after implementation completion (as described in the applicable SOW).

Minimum Monthly User: The minimum commitment that Customer has committed to, as set forth in the Services Order.

Named User: A billable named user is anyone that has logged in to the PureConnect service at least once during the billing period.

Ramp Period: The optional period of time (shown in the Services Order), during which Customer will transition to Full Production. The default Ramp Period is zero (0) days if not specified. The Ramp Period will begin on the Live date.

Reports: operational and historical reports provided to Customer through a standard set of reporting templates or widgets, configured by Customer personnel, or developed by Licensor PS pursuant to a statement of work.

User: An individual who (i) is authorized by Customer; and, (ii) has been supplied a user identification and password(s) by Customer to access the Genesys Cloud Services on Customer's behalf. A User may be a Concurrent User or Named User, as described in the Services Order.

Exhibit A

PureConnect Support Policy

1. ***Support Incident Priority Levels***

Incidents will be categorized and handled according to an assigned severity level. The assigned severity level for a problem may be mutually determined by both parties during the problem resolution process, but Licensor shall have final authority as to the actual designation Licensor uses commercially reasonable efforts to respond to each Support incident within the applicable response time and reach resolution of code red and high impact issues within the timeframes described in the table below.

PRIORITY LEVEL	INITIAL RESPONSE	MEAN TIME TO RESTORATION (MTTR)
Code Red	15 minutes (by Phone)	15 minutes
High	15 minutes (by Phone)	72 hours
Medium	24 hours (by Web)	N/A
Low	2 business days (by Web)	N/A

Upon Customer request and with Customer cooperation, Licensor will make administrative moves, additions and/or changes (MACs) as follows:

a. The MAC will be scheduled during posted business hours and will be completed within twenty-four (24) business hours after receipt of the request.

b. Customer will pay the amounts stated in the *Order Form* for MACs.

2. ***PureConnect Service Levels***

a. "Hard Outage" means that the PureConnect Services cannot receive and route calls or place calls with the primary server, switchover server or via remote survivability. ""Planned Outage" and "Emergency Maintenance" mean downtime in the PureConnect Services for scheduled maintenance.

b. Excluding Planned Outages and Emergency Maintenance, commercially reasonable efforts will be used to provide at least 99.99% uptime of the PureConnect Services to support incoming and outgoing calls, three-hundred and sixty-five (365) days a year, twenty-four (24) hours a day. If the PureConnect Services do not meet the foregoing standards, Licensor will issue a Hard Outage credit to Customer equal to the applicable Credit Percentage shown below multiplied by the Monthly Cost of the Minimum Monthly Commitments for Genesys Software specified within the Order Form for the affected PureConnect Services:

PURECONNECT SERVICE UPTIME PERCENTAGE		CREDIT PERCENTAGE
Less than 99.99%	To 99.97%	1%
Less than 99.97%	To 99.90%	3%
Less than 99.90%	To 99.25%	5%
Less than 99.25%	To 98.00%	10%
Less than 98.00%		20%

PURECONNECT I/O SERVICE UPTIME PERCENTAGE		CREDIT PERCENTAGE
Less than 99.99%	To 99.975%	1%
Less than 99.975%	To 99.900%	3%
Less than 99.900%	To 99.250%	5%
Less than 99.250%	To 98.000%	10%
Less than 98.000%		20%

c. The Uptime Percentage equals (1-(Total Minutes of Hard Outage/(# days in the month *1440)).

d. Code Red incidents due to customer managed equipment and/or applications (email server, web chat server, etc.) are excluded from Hard Outage credits.

e. In order to receive any Hard Outage credit, Customer must request the credit no later than thirty (30) days after the end of the month during which the credit was earned and must not be past due on any invoices. Customer will not be entitled to the Hard Outage credit if the failure was not caused by Genesys, including without limitation, failures caused by: (i)

interruption in data or voice service (local or long distance) regardless of whether the provider is contracted by Licensor, Genesys, or by Customer; (ii) Customer's internet connection, network, equipment, software (other than Interface Software), facility, databases or operator error; and (iii) alterations, modifications, configurations, or customizations of the Services, other than those undertaken and performed by Genesys. The Hard Outage credit is the Customer's sole remedy for any failure to meet the PureConnect Service Level standards.

3. ***Support Policies***
Additional support policies, procedures, and services will be described in the Customer Handbook. Genesys may modify this Support and Service Level Policy (any websites referenced in this EUA) at any time by posting a revised version on the website and by otherwise notifying Licensor and/or Customer. The modified terms will become effective upon posting or, if notified by email, as stated in the email message. By continuing to use the PureConnect Service after the effective date of any modifications to this EUA, Customer agrees to be bound by the modified terms. If such modification materially decreases any of Licensor or Genesys's obligations or the functionality of the PureConnect Service, Customer may terminate this EUA. Neither Licensor nor Genesys will have any obligation to take any action to correct a problem reported by Customer if Licensor or Genesys determines that the problem: (i) arises from use of the PureConnect Services or Interface Software contrary to this Support and Service Level Policy or the documentation regarding the service provided to Customer by Genesys; (ii) arises from Customer's use of the PureConnect Services or Interface Software in combination with equipment or third party software not certified by Genesys for use in combination with the PureConnect Services and Interface Software; or (iii) is not included in standard support services as defined in the PureConnect Customer Guide. Support will be provided by telephone, web ticketing and remote access and does not include support at any Customer Site.

4. ***Equipment Maintenance***.
Licensor's support obligations include: (i) initial troubleshooting and issue isolation for issues with all Equipment used to provide the Genesys PureConnect Cloud Service, and (ii) maintenance services (installing version upgrades and patches) for the Genesys proprietary software on such Equipment. However, Customer is responsible for: (i) assisting Licensor and Genesys in troubleshooting and issue isolations for issues with Equipment on Customer's site(s) or any Equipment controlled by customer in Genesys' data centers (collectively "Customer-controlled Equipment"), and (ii) any software or hardware maintenance other than the Genesys proprietary software (examples: operating system, antivirus, etc.) on Customer-controlled Equipment. Customer must ensure all Customer-controlled Equipment is compatible with all new versions of the Genesys proprietary software.

5. ***After Hours Support***
After Hours support is subject to an additional charge of $250 per incident. A support request shall be considered After Hours if the support request is non-Critical and made on a holiday or outside the hours identified in Customer Handbook. Unless otherwise identified on the *Order Form*, Customer Time Zone shall be the time zone of the primary PureConnect data center serving the Customer.

6. ***System Maintenance***
Refers to any system or infrastructure impacting change or update that has the potential to result in a brief momentary loss, impact, or reduction to the resiliency or functionality of the PureConnect Service.

    a. **Planned Maintenance** – Planned maintenance shall not involve any activity that is anticipated to have a material or adverse effect on the live, operational functioning of the PureConnect Services.

Advanced notice will be provided prior to any planned maintenance event. Planned maintenance will be performed between the hours of 12:00 A.M. and 5:00 A.M. within the time zone of the Customer's primary PureConnect data center.

b. **Planned Outage** – Planned outages involve any activities (operating system patches, service updates, equipment reboot etc…) which are anticipated to cause interruption to the operational functioning of the PureConnect Services.

   Advanced posted notification will be provided prior to conducting any planned outage. Planned outages will be scheduled between the hours of 12:00 A.M. and 5:00 A.M. within the time zone of the Customer's primary PureConnect data center.

c. **Emergency Maintenance** – Emergency maintenance involves any activity (operating system patches, service updates, equipment reboot etc…) where Genesys may or may not be to anticipate an interruption to the operational functioning of the PureConnect Services.

   Due to the potential urgent nature of this type of maintenance, it is not always possible to perform emergency maintenance during normal maintenance periods.

7. ***Termination for Cause***

   a. Customer may terminate this EUA for cause and without penalty if Customer experiences a failure of the PureConnect Services resulting in an Uptime Percentage of less than 98.000% in three (3) months during a rolling twelve (12) month period and, within thirty (30) days of such occurrence, Customer gives Licensor and Genesys at least thirty (30) days written Notice of termination.

8. ***Network Assessment***

For any VoIP implementation, Customer's network must meet the following standards:

a. Quality of Services ("QoS") must be enabled on all VoIP-related network devices and endpoints and configured in accordance with the QoS for the xIC Platform whitepaper.

b. Full Duplex must be enabled on all network devices.

c. RTP latency in one direction must be less than 150 ms for voice traffic.

d. RTP jitter must be less than 30 ms.

e. RTP packets must include highest markings for service priority queuing (ex. DSCP for Cisco devices).

f. Network segments must not exceed a packet loss rate of one percent (1%).

g. Network bandwidth must accommodate approximately 88kb/s for calls using audio codec G711 and 32kb/s for calls using audio codec G729 (not including overhead for VPN encryption/decryption, if applicable).

h. VLAN settings must be set in accordance with the QoS for the xIC Platform whitepaper.

If Licensor or Genesys determines that Customer's network does not meet these standards, Customer must rectify the failures. Customer will not be entitled to receive Hard Outage credits unless and until Customer's network meets these standards.At any time if it is reasonably determined by Licensor or Genesys that Customer's network does not meet these standards, then any support provided as a result of the network inadequacy will be provided at the rates stated in the Order Form.

9. ***Reports***
   Licensor will provide an automated report to Customer within five (5) days after the end of each month showing all support incidents opened during that month including: (a) the incident number; (b) the date and time the incident was opened; (c) the Customer Site impacted; (d) close date/time for the fix or work-around; (e) the total Hard Outage time.

Definitions

Code Red – PureConnect's operational ability to receive, route and deliver Customer purchased interaction services is 'down', severely degraded, or major components of the service are not operational and work cannot reasonably continue for greater than 10% of minimum monthly agent commitment as identified in the Order Form (see column entitled "Minimum Monthly Commitment for Users/Item"). Interaction services which are 'down' or severely degraded due to Customer managed equipment and/or applications (email server, web chat server, etc.) are excluded from 'Hard Outage credits.

High – Non-business critical features of the PureConnect Services are impaired or non-functional (for example: Interaction Supervisor, Interaction Recorder).

Medium – Non-disabling or cosmetic errors with little or no impact on the PureConnect Services.

Low – Requests for information on PureConnect Services, Policies, Processes, or Procedures from Supplier by members of Customer's Business, Management, or technical staff teams.

Initial Response – The difference between the time an automated alert or Customer support request (phone or web ticket) is received by Licensor and the time it is assigned to a PureConnect Support representative within the service management system.

Mean Time to Restoration (MTTR) – Average duration of the outage from the time of an automated alert or customer reported incident.

Exhibit B

PureConnect Security Policy

This security policy describes the minimum requirements for information security and data protection provided in relation to the provision of Genesys PureConnect Cloud Services under this EUA. This security policy is applicable only to the extent that Genesys has access and control over Customer Data. For the purposes of this Exhibit B, "Data Center" means a data center where Genesys houses servers and other components used to deliver the Genesys PureConnect Cloud Service.

1 SECURITY PROGRAM

1.1 Security Certifications. Genesys has 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 Genesys PureConnect Cloud Services provided. Genesys has developed and will maintain an information security and awareness program that is delivered to all its 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.
1.2 Security Awareness and Training. Genesys has developed and will maintain an information security and awareness program that is delivered to all 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.
1.3 Policies and Procedures. Genesys will maintain appropriate policies and procedures to support the information security program. Policies and procedures will be reviewed annually and updated, as necessary.
1.4 Change Management. Genesys will utilize a change management process based on industry standards to ensure that all changes to Customer's environment are appropriately reviewed, tested, and approved.
1.5 Data Storage and Backup. Genesys will create backups of critical Customer Data according to documented backup procedures. Customer Data will be stored and maintained solely on designated backup storage media within the Data Center(s). Backup data will not be stored on portable media. Customer Data stored on backup media will be protected from unauthorized access. Backup data for critical non-database production servers will be retained for approximately thirty (30) days. Backup data for critical production database servers and transactional data will be retained for a minimum of seven (7) days.
1.6 Anti-Virus and Anti-Malware Protection. Genesys will utilize industry standard anti-virus and anti-malware protection solutions to ensure that all servers in Customer's Genesys PureConnect Cloud Service environment are appropriately protected against malicious software such as trojan horses, viruses, and worms. The solution will be centrally managed and configured to ensure updates are applied in a timely manner. Genesys will use standard industry practice to ensure that the Genesys PureConnect Cloud Services as delivered to Customer does not include any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan Horses) that are designed to disrupt the proper operation of the Genesys PureConnect Cloud Services, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause the Genesys PureConnect Cloud Services to be destroyed, damaged, or rendered inoperable. Customer acknowledge that the use of license keys will not be a breach of this section.
1.7 Penetration Testing. On at least an annual basis, Genesys will conduct a vulnerability assessment and penetration testing engagement with an independent qualified vendor. Issues identified during the engagement will be appropriately addressed within a reasonable time-frame commensurate with the identified risk level of the issue. A cleansed version of the executive summary of the test results will be made available to Customer upon written request and will be subject to non-disclosure and confidentiality agreements.
1.8 Vulnerability and Patch Management. Genesys will maintain a vulnerability management program based on industry standard practices that routinely assesse the Data Center environment. Routine network and server scans will be scheduled and completed on a regular basis. The scan results will be analyzed to confirm identified vulnerabilities, and remediation will be scheduled within a timeframe commensurate with the relative risk. Genesys will monitor a variety of vulnerability advisory services to ensure that newly identified vulnerabilities are appropriately evaluated for possible impact to the Genesys PureConnect Cloud Service. Critical and high-risk vulnerabilities will be promptly addressed following the patch management and change management processes.
1.9 Data Destruction. Genesys will follow industry standard processes for the secure destruction of Customer Data that becomes obsolete or is no longer required under the Agreement. Retired or decommissioned equipment that

formerly held Customer Data and is scheduled for destruction will be securely destroyed using a qualified vendor who will provide a certificate of secure destruction.

2 NETWORK SECURITY

2.1 Network Controls. Genesys will employ effective network security controls based on industry standards to ensure that Customer Data is segmented and isolated from other customer environments within the Data Center. Controls include, but are not limited to:
A) Segregated Firewall Services. Customer environments are segmented using physical and contextual firewall instances.
(B) Network-Based Intrusion Detection System (NIDS). Genesys has implemented industry standard network intrusion detection systems at Internet egress points across the Genesys PureConnect Cloud Service environment.
(C) No Wireless Networks. Wireless networks are not utilized within the Data Center environments.
(D) Data Connections between Customer and the Genesys PureConnect Cloud Service Environment. Genesys uses SSL/TLS and/or MPLS circuits to secure connections between browsers, client apps, and mobile apps to the Genesys PureConnect Cloud Service. Connections traversing a non-dedicated network (i.e. the Internet) will use SSL/TLS.
(E) Data Connections between Genesys PureConnect Cloud Service Environment and Third Parties. Transmission or exchange of Customer Data with Customer and any third parties authorized by Customer to receive the Customer Data will be conducted using secure methods (e.g. SSL/TLS, HTTPS, SFTP).
(F) Encrypted Recordings. Genesys encrypts call recordings and chat sessions. Customer may elect to implement a unique password, known only to Customer, to protect the encryption keys used to secure the call recordings and chat sessions.
(G) Encryption Protection. Genesys uses industry standard methods to support encryption. For asymmetric key encryption, Genesys uses RSA 2048 bit keys. For symmetric key encryption, Genesys uses AES-128 bit keys. For hashing, Genesys uses SHA1 and SHA2.
(H) Logging and Monitoring. Genesys will log security events from the operating perspective for all servers providing the Genesys PureConnect Cloud Service to Customer. Genesys will monitor and investigate events that may indicate a security incident or problem. Event records will be retained for ninety (90) days.

3 USER ACCESS CONTROL

3.1 Access Control. Genesys will implement appropriate access controls to ensure only authorized users have access to Customer Data within the Genesys PureConnect Cloud Service environment.
3.2 Customer's User Access. Customer is responsible for managing user access controls within the application. Customer defines the usernames, roles, and password characteristics (length, complexity, and expiration timeframe) for its users. Customer is entirely responsible for any failure by itself, its agents, contractors or employees (including without limitation all its users) to maintain the security of all usernames, passwords and other account information under its control. Except in the event of a security lapse caused by Genesys' gross negligence or willful action or inaction, Customer is entirely responsible for all use of the Genesys PureConnect Cloud Service through its usernames and passwords whether or not authorized by Customer and all charges resulting from such use. Customer will immediately notify Genesys if Customer becomes aware of any unauthorized use of the Genesys PureConnect Cloud Service.
3.3 Genesys User Access. Genesys will create individual user accounts for each of its employees or contractors that have a business need to access Customer Data or Customer systems within the Genesys PureConnect Cloud Service environment. The following guidelines will be followed with regard to Genesys user account management:
(A) User accounts are requested and authorized by Genesys management.
(B) Strong password controls are systematically enforced.
(C) Connections are required to be made via secure VPN using strong passwords that expire every ninety (90) days.
(D) Dormant or unused accounts are disabled after ninety (90) days of non-use.
(E) Session time-outs are systematically enforced.
(F) User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

4 BUSINESS CONTINUITY AND DISASTER RECOVERY

4.1 Disruption Protection. The Genesys PureConnect Cloud Service will be deployed and configured in a high-availability design and the Genesys PureConnect Cloud Service will be deployed across geographically separate Data Centers to provide optimal availability of the Genesys PureConnect Cloud Service. The Data Center environment is physically separated from the Genesys corporate network environment so that a disruption event involving the corporate environment does not impact the availability of the Genesys PureConnect Cloud Service.
4.2 Business Continuity. Genesys 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.
4.3 Disaster Recovery. The Genesys PureConnect Cloud Service will be deployed in a high-availability, geographically redundant design such that a disruption event at a single Data Center will trigger a system fail-over to the back-up Data Center to minimize disruption to the Genesys PureConnect Cloud Service. Customer is responsible for defining specific parameters regarding fail-over.

5 SECURITY INCIDENT RESPONSE

5.1 Security Incident Response Program. Genesys will 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.
5.2 Notification. In the event of a confirmed breach involving the unauthorized release or disclosure of Customer Data or other security event requiring notification under applicable law, Genesys will notify Customer within seventy-two (72) hours and will reasonably cooperate so that customer can make any required notifications in connection with such event, unless Genesys is specifically requested by law enforcement or a court order not to do so.
5.3 Notification Details. Genesys 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 Genesys; (iv) corrective measures to be taken; and (v) evaluation of alternatives and next steps.
5.4 Ongoing Communications. Genesys will continue providing appropriate status reports to Customer regarding the resolution of the Security Incident, continually work in good faith to correct the Security Incident and to prevent future such Security Incidents. Genesys will cooperate, as reasonably requested by Customer, to further investigate and resolve the Security Incident.

6 DATA CENTER PROTECTIONS

6.1 Data Center Co-Location. Genesys contracts with third-party providers for Data Center colocation space. Data Center providers and related services are reviewed on an annual basis to ensure that they continue to meet the needs of Genesys and its customers. Each Data Center provider maintains certification based on their independent business models. Security and compliance certifications and/or attestation reports for the Data Center(s) relevant to Customer's Genesys PureConnect Cloud Service will be provided upon written request and may require additional non-disclosure agreements to be executed.
6.2 Physical Security. Each Data Center is housed within a secure and hardened facility with the following minimum physical security requirements: (a) secured and monitored points of entry; (b) surveillance cameras in facility; (c) on-site access validation with identity check; (d) access only to persons on an access list approved by Genesys; (e) on-site network operations center staffed 24x7x365.
6.3 Environmental Controls. Each Data Center is equipped to provide redundant external electrical power sources, redundant uninterruptible power supplies, backup generator power, and redundant temperature and humidity controls.

7 RIGHT TO AUDIT

7.1 Customer or its designated representative will have the right to audit Genesys records and systems related to the performance of the Genesys PureConnect Cloud Service under this Agreement, upon thirty (30) business days' prior written notice. Genesys agrees to cooperate in good faith with Customer to determine and implement a mutually agreeable resolution to any significant concerns identified during any such audit. Any audits performed by Customer

or its designated representatives under this Agreement will be conducted a maximum of one (1) time during any twelve (12) month period during which this Agreement remains in force. Audits will be conducted during normal business operating hours and will be conducted in a manner that minimizes any disruption to Genesys normal daily operations.

8 PRIVACY

8.1 Genesys has developed and will maintain a privacy program designed to respect and protect Customer Data under our control. Genesys will not rent, sell or otherwise share any Customer Data with outside parties. Customer Data will only be used or accessed for providing the Genesys PureConnect Cloud Service.

9 INDUSTRY SPECIFIC CERTIFICATIONS

9.1 Genesys security and operational controls are based on industry standard practices. Genesys will configure the solution and the Genesys PureConnect Cloud Service based on Customer's specifications as defined in a mutually agreed upon Statement of Work (SOW); however, Customer is solely responsible for achieving and maintaining any industry specific certifications required for its business (e.g. PCI DSS, HIPAA, GLBA, NIST 800-53, FedRAMP, etc.).

10 PREMIUM SERVICES

10.1 Additional Services. The standard security controls listed prior to this Section 10 meet industry standards and are sufficient for most customers. Customers requiring a higher level of assurance may need to contract for additional "Premium Services" as described in this Section 10. If an industry specific certification is required for Customer's business relative to the Genesys PureConnect Cloud Service, Customer agrees to contract for the additional "Premium Services" required to meet the industry specific certification. For an additional fee, Genesys will implement the following controls and procedures during the implementation period. The controls and procedures are designed to meet the certification requirements of certain industry standards (PCI DSS, HIPAA, etc.) where appropriate for Customer Genesys PureConnect Cloud Service environment within the Data Center. Additional controls may include, but may not be limited to:
(A) Remote Access. Genesys authorized employees and contractors will require two-factor authentication to access Customer's Genesys PureConnect Cloud Service environment within the Data Center.
(B) Vulnerability and Patch Management. Genesys will conduct quarterly vulnerability scans of Customer's Genesys PureConnect Cloud Service environment within the Data Center. Critical and high-risk vulnerabilities will be addressed, following the documented change management and patch management procedures. Medium and lower risk vulnerabilities will be remediated.
(C) Logging and Monitoring. Genesys will conduct reviews of infrastructure event logs daily. Identified issues and concerns will be risk ranked and addressed according to documented vulnerability management procedures.
Certification Audits. Genesys will contract with qualified third-party assessors to conduct industry specific certification audits of the Genesys PureConnect Cloud Service within the Data Center. Certification audits will be conducted on an annual basis. The resulting certification or executive summary of the audit report will be provided to Customer upon written request. Genesys currently maintains PCI DSS 3.2 certification for a specific deployment model within the U.S. Data Centers located in Carmel, Indiana and Englewood, Colorado and within the EMEA Data Centers located in Frankfurt, Germany and Slough, UK. PCI certification does not extend to any other Data Center.