AWS Acceptable Use Policy

Last Updated: July 1, 2021

This Acceptable Use Policy ("**Policy**") governs your use of the services offered by Amazon Web Services, Inc. and its affiliates ("**Services**") and our website(s) including http://aws.amazon.com ("**AWS Site**"). We may modify this Policy by posting a revised version on the AWS Site. By using the Services or accessing the AWS Site, you agree to the latest version of this Policy.

You may not use, or facilitate or allow others to use, the Services or the AWS Site:

- for any illegal or fraudulent activity;
- to violate the rights of others;
- to threaten, incite, promote, or actively encourage violence, terrorism, or other serious harm;
- for any content or activity that promotes child sexual exploitation or abuse;
- to violate the security, integrity, or availability of any user, network, computer or communications system, software application, or network or computing device;
- to distribute, publish, send, or facilitate the sending of unsolicited mass email or other messages, promotions, advertising, or solicitations (or "spam").

Investigation and Enforcement

We may investigate any suspected violation of this Policy, and remove or disable access to any content or resource that violates this Policy in accordance with the Contract Disputes Act. You agree to cooperate with us to remedy any violation.

When determining whether there has been a violation of this Policy, we may consider your ability and willingness to comply with this Policy, including the policies and processes you have in place to prevent or identify and remove any prohibited content or activity.

Reporting of Violations

To report any violation of this Policy, please follow our abuse reporting process.

Genesys Cloud Service Level Agreement

Overview

Scope. This Genesys Cloud Service Level Agreement ("SLA") is a policy governing the use of the Genesys Cloud Service, and is made part of the Genesys Cloud Terms and Conditions (or other master agreement governing Customer's use of the Genesys Cloud Service entered into between the parties)(the "Agreement"). In the event of a conflict between the terms of this SLA and the terms of the Agreement, the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

Provision of Service. Genesys will make the Genesys Cloud Service available 24 hours a day, 7 days a week, and use commercially reasonable best efforts to provide 100% uptime, except for any unavailability caused by circumstances beyond Genesys' reasonable control, including failure or delay of Customer's Internet connection, misconfiguration by Customer or any third party acting on Customer's behalf, issues on Customer's network, or telecommunications services contracted directly by Customer (collectively, "Uptime Exclusions").

Severity levels

Severity and Priority. "Severity" is defined as the impact that an issue has on the Customer's ability to conduct business. Issue severity levels are defined below. "Priority" is defined as the customer-designated level of importance.

Issue Severity Levels. The Severity levels assigned to an issue are defined as follows:

Issue severity	Definition
1 - Critical impact (Code Red)	Customer is experiencing a severe problem resulting in an inability to perform a critical business function. There is no workaround.
2 - High impact	Customer is able to perform job functions but performance is degraded or limited.
3 - Medium impact	Customer's ability to perform job functions is largely unaffected, but noncritical functions or procedures are unusable or hard to use. A workaround is available.

Issue severity	Definition
4 - Low impact	The Genesys Cloud Service is available and operational; trivial impact to Customer's business operations or Customer requires information or assistance on the Genesys Cloud Service capabilities or configuration.

Designated Contact. Customer must designate a primary contact, and at least one backup in the primary's absence, to act as a primary liaison between Customer and the Genesys Cloud Service customer care team (the "Designated Contact"). The Designated Contact must be knowledgeable about the Genesys Cloud Service and will participate in troubleshooting support cases.

Preliminary Troubleshooting. When a Customer becomes aware of an issue, prior to opening a support case with Genesys, the Designated Contact must perform reasonable basic troubleshooting and use best efforts to understand the Customer's areas of responsibility, as described on Genesys' support portal.

Case Submission. Cases for all Severity levels, except Critical Impacting cases, may be raised by Customer by either phone or through the support portal. Issues designated by Customer as Critical Impact must be raised by telephone through the applicable Genesys customer care number found on the support portal. If a case has been submitted through the support portal and the business impact has increased to Critical Impact severity, Customer must request critical support for the case by telephone. Submission of cases on the support portal will include the Customer name, Customer organization ID, and a description of the use and its business impact. The Designated Contact will include any other information known by the Designated Contact that is reasonably helpful for Genesys to analyze the issue (example: environmental changes including network or firewall changes, new configurations, previous troubleshooting efforts, etc.).

Severity Assignment. Genesys' customer care team prioritizes issues based on the severity level. When a case is opened by Customer, Customer will identify a Priority based on the descriptions in the table above. Customer's Priority designation will be used as a factor by Genesys when defining the Severity of an issue. The assigned Severity level for an issue may be mutually redetermined by both Genesys and Customer during the issue resolution process. Both parties agree to act reasonably in making in such determination.

Target initial response times

Target initial response times are based on the Severity level of each incident. The automated response received by Customer following submission of the case will not be deemed to be Genesys' initial response. The initial response is deemed to have been made

when the issue has been assigned to the appropriate Genesys personnel, and Customer receives a human response (by phone or case notes message) from Genesys acknowledging the issue. Genesys will use reasonable efforts to respond to issues in accordance with the table below:

Severity level	**Target initial response time**
1 - Critical impact (Code Red)	Customer is experiencing a severe problem resulting in an inability to perform a critical business function. There is no workaround. Response target: 10 min. (phone)
2 - High impact	Customer is able to perform job functions but performance is degraded or limited. Response target: 2 hours (My Support)
3 - Medium impact	Customer's ability to perform job functions is largely unaffected, but noncritical functions or procedures are unusable or hard to use. A workaround is available. Response Target: 2 hours (My Support)
4 - Low impact	The Genesys Cloud Service is available and operational; trivial impact to Customer's business operations or Customer requires information or assistance on the Genesys Cloud Service capabilities or configuration. Response Target: 2 hours (My Support)

SLA credits

Uptime. "Uptime" is defined as the percentage of time during a month (not including Uptime Exclusions) in which all Genesys Cloud functionality necessary to perform real-time interactions between Customer and its customers/clients (e.g. inbound voice, outbound voice, IVR routing) are accessible. Uptime percentage is calculated as follows: Uptime = (A-B+C)/A; where A = total time in the month, B = time during the month in which critical business functions are not accessible, and C = time of Uptime Exclusions during the month.

Credits. If the Genesys Cloud Service Uptime falls below the thresholds in the table below in any one-month billing cycle, Customer will be entitled to the credits defined below. The applicable credit is a percentage of Customer's monthly committed Subscription Fees as defined in the Service Order and is applicable only to Annual Prepay or Annual Month to

Month contracts. The percentage applies to either the monthly committed Subscription fees, or if paid annually the annual minimum committed Subscription Fees, pro-rated for a one-month period.

Uptime %	**Credit %**
Below 99.99%	10%
Below 99.0%	30%
Below 97%	100%

Credit Requests and Payment. Customer must request a credit within thirty (30) days after the month in which the uptime fell below one of the foregoing thresholds and have a support case created for the incident which validates the impact caused. Customer must contact its Genesys customer success manager to request the credit. Upon Customer's valid request, Genesys will apply the applicable credit to the following month's invoice. If Customer is on an annual pre-payment structure, Genesys will provide the applicable credit as a credit to the prepaid balance or a credit refund, at Customer's discretion.

Cooperation

Customer acknowledges that Genesys' customer care team may need to be able to reproduce errors in order to resolve them. Customer will cooperate and work closely with Genesys to reproduce errors, including conducting diagnostic or troubleshooting activities as requested and appropriate. Also, subject to Customer's approval on a support case-by-support case basis, Users may be asked to provide remote access to their Genesys Cloud application and/or desktop system for troubleshooting purposes.

GENESYS CLOUD SERVICES END USER AGREEMENT

This Genesys Cloud Services End User Agreement and the documents referenced herein (the **"Agreement")** is entered into by and between the Genesys Reselling Partner entity ("**Supplier**") and the counterparty to a Services Order(s) for Cloud Services referencing this Agreement (**"Customer"**) and contains the terms and conditions that govern Customer's access to and use of the Cloud Services (as defined below).

This Agreement takes effect when both parties have executed the Services Order (**"Effective Date"**). The person legally agreeing to this Agreement represents to Supplier that they are lawfully able to enter into contracts that bind the entity they represent and that they have legal authority to do so.

1. DEFINITIONS

Affiliate: a business entity that: (i) Controls the subject party; (ii) is Controlled by such party; or (iii) is under common Control with such party, but only during the time that such Control exists. "**Control(led)**" is the ability to determine the management policies of an entity through equity ownership of a majority of interests of such entity.

AWS Region: as defined and listed at https://aws.amazon.com/about-aws/global-infrastructure/regions_az/.

Cloud Services: Genesys-operated cloud offerings that are based on Genesys' proprietary software deployed in a Genesys-managed cloud services environment, the specific features and functionality of which are described in the Documentation and identified on a Services Order as being part of the Cloud Services. Cloud Services exclude Third-Party Products and PS Apps.

Confidential Information: proprietary or other information which can reasonably be considered confidential due to its nature, or is marked as confidential, and any third-party confidential information, provided by one party (**"Discloser"**) to the other party hereto (**"Recipient"**).

Customer Data: Customer's and Customer's customers' Confidential Information that is inputted and stored in the Cloud Services. Customer Data does not include the anonymized data incorporated into Service Improvements as defined in Section 9.3.

Documentation: the applicable technical instructions describing the operation of the Cloud Services found at https://help.mypurecloud.com/solutions-subscriptionplans-licensing-and-pricing-home/.

Materials: Cloud Services and Documentation, collectively.

PS Apps: any Genesys-developed application sold separately as an add-on to the Cloud Services, including but not limited to any such application available on Genesys' online marketplace located at http://appfoundry.genesys.com ("**AppFoundry**"), which may be subject to additional terms and conditions.

Services: Cloud Services and the additional services listed in Section 2.5.1.

Services Order: the document by which Customer orders Cloud Services pursuant to this Agreement.

Third-Party Product: any software or service proprietary to an entity other than Genesys or its Affiliates that (i) is sold or licensed separately from a standard Cloud Services license, (ii) may integrate or interoperate with the Cloud Services, and (iii) is accessible through AppFoundry or a third party provider.

2. ACCESS RIGHTS AND ADDITIONAL TERMS

2.1 **Access Rights**. Subject to the terms and conditions of this Agreement, Supplier grants Customer a non-exclusive, non-transferable, revocable, worldwide right to authorize individuals within Customer's organization, its Affiliates and contractors to use and access the Materials solely for Customer's internal business purposes during the Subscription Term. Customer is responsible for its Affiliates' and its contractors' compliance with the terms of this Agreement and use of the Materials. Customer has no right to receive a copy of the object code or source code versions of the Cloud Services.

2.2 **Continuous Delivery**. Genesys continuously releases usability enhancements, patches, and other updates for Cloud Services. The Documentation is regularly updated by Genesys to reflect changes to Cloud Services. Customer can subscribe to notifications about new releases under https://help.mypurecloud.com/subscribe-to-genesys-cloud-release-notes//.

2.3 **Support and Security.** Supplier will provide support for the Cloud Services as set forth in a separate agreement. The Service Level Agreement applicable to the Cloud Services is attached hereto and set forth at https://help.mypurecloud.com/articles/service-level-agreements/, and security for the Cloud Services will be provided in accordance with the terms attached hereto and at https://help.mypurecloud.com/articles/genesys-cloud-security-policy/, which terms are incorporated herein by reference. Customer may subscribe to notifications about changes to the abovementioned terms under https://help.mypurecloud.com/subscribe-to-tc/ and https://help.mypurecloud.com/articles/genesys-cloud-security-policy/.

2.4 **Updates.** Genesys reserves the right to non-materially update the terms incorporated into Sections 2.2 and 2.3 during the Subscription Term. Such updates will become effective upon posting. If, however, such a change results in the material degradation of the functionality of the Cloud Services, the level of support for the Cloud Services, or the security of Customer Data and no workaround has been provided by Supplier, or its licensor, Genesys, then Customer may terminate any affected Services Order by providing Supplier with written notice within 30 days from publication of such change, upon which Supplier will refund any pre-paid, unused fees to the Customer.

2.5 **Terms Applicable to Third Party Products, Additional Services, and Country Specific Provisions.**

2.5.1 Customer's use or Genesys' provision of any Third-Party Products may be accompanied by terms of the shrink-wrap, click-wrap or other accompanying license included or provided with such Third-Party Products. Neither Supplier, nor its licensor, Genesys, shall have any liability or additional obligations to Customer in connection with Third-Party Products. Further, additional services, such as professional services, Genesys Beyond training courses, Genesys Pointillist Services, Genesys Analytics Add-on Services, and / or Genesys Cloud Voice subject to additional terms that Supplier will provide if ordered.

2.5.2 Additional country-specific provisions will apply to Customer or Customer's Affiliates when accessing the Cloud Services from any of the countries identified in the Country Specific Term Schedule, included herein.

3. RIGHTS AND LIMITATIONS OF USE

3.1 **Proprietary Rights**. All intellectual property rights in the Materials, and all updates, upgrades, enhancements, new versions, releases, corrections, copies, translations, adaptations, and modifications thereof, are and shall remain the exclusive property of Genesys or its Affiliates, business partners, licensors or suppliers, as applicable, whether or not specifically recognized or perfected under applicable laws. All intellectual property rights in and to Customer Data are and shall remain Customer's sole property, provided, however, that Customer grants Supplier, Genesys, and its Affiliates and contractors the right to access, process, store, transmit, and otherwise make use of the Customer Data with the Cloud Services to ensure its proper operation, fulfil Supplier's and Genesys' obligations, or as otherwise consistent with this Agreement. Genesys will not rent or sell Customer Data.

3.2 **Use Restrictions**. Customer will not, and will not permit, or authorize any third party to, (i) sell, rent, lease, transfer, sublicense, share or otherwise make the Materials available to any third party, except as expressly authorized by this Agreement; (ii) create any derivative works, functionally equivalent product(s) or translations of the Cloud Services, or otherwise use the Materials other than as expressly permitted by this Agreement; (iii) copy any feature, design or graphic in, or disassemble, reverse engineer or decompile, the Cloud Services; (iv) access or use the Materials to compete with Genesys or to assist a third party to do so; (v) remove or modify any proprietary markings or restrictive legends placed on the Materials; (vi) take any action that jeopardizes Genesys' rights or that of its Affiliates, business partners, licensors or suppliers in the Materials; (vii) violate any laws; (viii) use the Cloud Services in a manner that is defamatory, harassing, hateful, infringing or otherwise causes damage or injury to any person or property, including to Supplier or Genesys and its Affiliates, business partners, licensors or suppliers; (ix) publish or disclose to any third parties the results of any performance, benchmarking or comparison testing, or analysis of the Genesys Cloud Services; (x) use the Materials to provide the following services to third parties, excluding Customer's Affiliates and contractors: outsourcing, hosting, application service provider or online services; (xi) transmit viruses or other deleterious code; (xii) perform unauthorized penetration testing, vulnerability scans, or automated testing; or (xiii) damage, disable, overburden, including load testing, or impair the Cloud Services or any other party's use of the Cloud Services.

3.3 **Feedback**. To the extent not already owned by Supplier's licensor, Genesys, Customer hereby grants Genesys a perpetual, exclusive, royalty-free, irrevocable, worldwide license to use or disclose any suggestions, enhancement requests, recommendations, proposals, ideas or other feedback Customer provides to Supplier or Genesys concerning the Services, and create derivative works thereof, without restriction, compensation, obligation or liability of any kind to Customer or to any third party.

3.4 **Data Center Services**. The software used to provide the Cloud Services is located on servers that are controlled by Amazon Web Services (**"AWS"**). AWS Acceptable Use Policy found at https://aws.amazon.com/aup/ (**"AWS AUP"**).

4. CONFIDENTIALITY

4.1 **Confidentiality**. Recipient will safeguard the confidentiality of Discloser's Confidential Information and will take, at a minimum, the precautions Recipient takes to protect its own Confidential Information but, in any event, no less than reasonable care. Recipient will (i) not disclose or use Discloser's Confidential Information for any purpose other than as contemplated by, and consistent with, the terms of this Agreement, (ii) limit access to Discloser's Confidential Information only to its Affiliates, employees and agents who have a need to know such information and who are bound by written confidentiality obligations at least as protective as this Agreement (provided Recipient shall be liable for such parties' compliance with the terms hereof), and (iii) not sell, transfer, disclose or otherwise make Discloser's Confidential Information available to any third party without Discloser's prior written consent.

4.2 **Disclosure Due to Binding Order**. If Recipient is required to disclose Discloser's Confidential Information to comply with a governmental or judicial order,

Recipient will promptly notify Discloser of such a request, unless legally prohibited from doing so, 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 may make the required disclosure if it is, upon the advice of counsel, compelled to disclose all or a portion of Discloser's Confidential Information. Genesys recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

4.3 **Exceptions**. 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) was 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 reliance on Discloser's Confidential Information. Genesys' Confidential Information includes the Materials, and other technical information relating thereto.

4.4 **Return and Retention of Confidential Information**. The Recipient will return any tangible materials containing Confidential Information, and any copies or reproductions thereof, to the Discloser within 30 days after the Discloser's written request; provided, however, the Recipient shall be permitted to retain copy of such Confidential Information for the purpose of performing any continuing obligations under this Agreement (including any Services Order), for archival purposes or compliance with applicable laws and regulations. Any Confidential Information retained by the Recipient shall be subject to confidentiality obligations pursuant to the terms of this Section. 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 Affiliates, employees, agents, or contractors.

4.5 **Reserved**.

5. WARRANTIES

5.1 **Cloud Services Warranty**. Subject to Section 5.2 (Warranty Exclusions), Supplier warrants to Customer that, during the Subscription Term, the Cloud Services will materially conform to the then-current description set forth in the Documentation. If Customer becomes aware of a warranty breach, Customer must notify Supplier in writing, upon which Supplier, or its licensor, Genesys, will, at its option, either: (i) modify the Cloud Services to materially conform to the current description; or (ii) provide a workaround solution that will reasonably meet Customer's requirements. If neither option is achieved or achievable within a reasonable period of time after Customer's written notification to Supplier, either party may terminate the affected Cloud Services by providing the other party 30 days' written notice of such termination and an opportunity to cure within such 30 days, after which termination will become effective and Supplier will refund any pre-paid, unused fees to the Customer. The remedies provided in this Section constitute Customer's sole and exclusive remedy for breach of the warranty described herein.

5.2 **Warranty Exclusions**. Supplier's, and its licensor, Genesys', warranties obligations set forth in this Agreement do not apply to the extent a warranty claim arises from: (i) Customer's use of the Services in combination with other programs, Third-Party Products, hardware, data or specifications that are not expressly described in the Documentation; (ii) Customer's use or configuration of Services contrary to the directions or descriptions in the Documentation; (iii) the development or use of any customizations, other than customizations undertaken and performed by Genesys, its subcontractors, or agents; or (iv) Customer Data or other Customer content uploaded to or used with the Services.

5.3 **Disclaimer. Except for the warranties expressly provided in this Section, the Materials are provided "as is" and Supplier and its licensor, Genesys, do not make, and hereby disclaim on behalf of itself, its licensor, Genesys, and its Affiliates, to the fullest extent permitted by law, all warranties, whether express or implied, statutory or otherwise, including any warranty of merchantability, satisfactory quality, fitness for a particular purpose, noninfringement, compatibility, security, timeliness, completeness, or accuracy. Without limiting the foregoing, Supplier and its licensor, Genesys, do not warrant that use of the Cloud Services will be uninterrupted or error free or that all defects will be corrected. To the extent that a warranty cannot be disclaimed as a matter of law, the scope and duration of such warranty will be the minimum permitted under applicable law.**

6. LIMITATION OF LIABILITY

6.1 **Unlimited Liability. The liability cap set forth in Section 6.2 and liability exclusions in Section 6.3 shall not apply to any liability resulting from: (i) Supplier's, or its licensor, Genesys', indemnification obligations for an IP claim as defined in Section 7.1; (ii)reserved; (iii) either party's breach of Section 4 (Confidentiality), except for breaches involving Customer Data, including security incident(s), which will be subject to Section 6.2; (iv) Customer's failure to pay any fees due under this Agreement, including any interest and/or collection costs; (v) either party's misappropriation of the other party's intellectual property rights; (vi) death or bodily injury; (vii) fraud or fraudulent misrepresentation; or (viii) any other liability which cannot be limited by operation of law.**

6.2 **Liability Cap. Subject to Sections 6.1 and 6.3 , the maximum aggregate liability of either party and its Affiliates to the other party and its Affiliates, collectively, for any and all event(s) giving rise to any liabilities, claims or causes of action arising in connection with or under this Agreement, including contract, warranty, tort (such as negligence), strict liability, misrepresentation, breach of statutory duty or otherwise, ("Event(s)"), will not exceed the total fees paid and payable by Customer to Supplier during the applicable Liability Period (as defined below). "Liability Period" means each 12 month period commencing on the Effective Date and on each anniversary thereafter. Any Event giving rise to separate causes of action will be considered a single Event and deemed to have occurred when the first Event occurred. If the Event occurs: (i) prior to execution of this Agreement, it shall be deemed to have occurred during the first 12 months of this Agreement, and (ii) after termination or expiration of this Agreement, it shall be deemed to have occurred during the last 12 months of this Agreement.**

6.3 **Liability Exclusions. Subject to Section 6.1, neither party nor its respective Affiliates will be liable to the other party for any: (i) indirect and/or consequential loss; (ii) special, incidental, exemplary, or punitive damages; (iii) loss of goodwill (including pecuniary losses arising from loss of goodwill); (iv) loss of profits or revenue; (v) loss of contract, sales and/or business; (vi) loss of savings, including anticipated savings; (vii) losses related to a disruption or work stoppage, cover damages (including the cost of procuring an alternative vendor, software or service); or (viii) wasted expenditure.**

6.4 **Risk Allocation. The limitations of liability and exclusions contained in this Agreement will apply regardless of (i) whether any resulting damages are foreseeable, and the legal theory asserted, and (ii) the success or effectiveness (or lack thereof) of any remedies provided herein. These limitations and exclusions are reflected in the pricing for the services made available hereunder, they represent an agreed-upon allocation of risk between the parties and are an essential part of this Agreement. Supplier and its licensor, Genesys, will not be liable for any damages caused by services provided free of charge. In the event that any exclusion or limitation of liability in this Section 6 is deemed unenforceable, limitation on liability will be the minimum amount permitted by law.**

7. INDEMNIFICATION

7.1 **Supplier IP Indemnification**. Subject to Section 7.2, Supplier, or its licensor, Genesys, will have the right to intervene to defend Customer from and against any third party claims alleging that the Cloud Services, in their unaltered state, infringes or misappropriates such third party's valid and enforceable intellectual property rights (**"IP Claim"**), and will indemnify Customer from damages finally awarded against Customer, and pay for any settlements agreed to by Supplier, or its licensor, Genesys, with respect to such IP Claims. Supplier, or its licensor, Genesys, may at any time and at its option and expense: (i) obtain for Customer a license to continue using the Cloud Services, (ii) modify the Cloud Services so as to avoid infringement while preserving substantially equivalent functionality, or (iii) terminate this Agreement or the applicable Services Order, and the rights granted thereunder, and refund to Customer any prepaid, unused fees covering the remainder of the Subscription Term of the applicable Services Order. This Section states Supplier's, and its licensor, Genesys', entire liability and Customer's sole and exclusive remedy with respect to any infringement or claims of infringement of any third-party intellectual property rights related to the Services. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

7.2 **IP Indemnification Exclusions**. Supplier's, and its licensor, Genesys', defense and indemnity obligations in Section 7.1 do not apply to the extent the IP Claim arises from: (i) third party products or Customer's use of the Cloud Services in combination with other programs, hardware, data or specifications that are not required by Genesys for the use of core functionality described in the Documentation; (ii) the development or use of any customizations, other than customizations undertaken and performed by Genesys, its subcontractors, or agents; (iii) Supplier's or its licensor, Genesys', compliance with Customer's request or instructions; (iv) Customer's way or process of doing business; or (v) Customer Data or other Customer content uploaded to or used with the Cloud Services.

7.3 **Reserved**. . Government shall be responsible for its use of the Services and for any damages or liabilities arising directly from such use, to the extent permitted by law and subject to the availability of appropriated funds, and in accordance with the Anti-Deficiency Act (31 U.S.C. §§ 1341, 1342, 1517). Nothing in this Agreement shall be construed as obligating the Government to any payment or financial obligation in advance of an appropriation therefor.

7.4 **Indemnification Procedures**. A party entitled to indemnification (**"Indemnified Party"**) will promptly notify the other party (**"Indemnifying Party"**) in writing of any claim and provide reasonable assistance to the Indemnifying Party with respect to handling such 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 has the right, at its sole discretion, 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 any such claim using counsel of its choice, at its own expense.

8. TERM. SUSPENSION OF SERVICES AND TERMINATION

8.1 **Term**. The term of this Agreement will start on the Effective Date and continue as set forth in the Services Order(s) (**"Term"**).

8.2 **Suspension**. Supplier, and its licensor, Genesys, reserve the right to immediately temporarily suspend the Cloud Services, or a portion thereof, or reject or cancel the transmission of any information through the Cloud Services based upon (i) reasonable belief that the use of the Cloud Services is in violation of laws, or (ii) an imminent compromise to the security or integrity of the network. As practicable depending on the circumstances, Supplier, or its licensor, Genesys, will provide notice of the suspension to Customer. Supplier, or it's licensor, Genesys, may also suspend the Cloud Services for Customer's failure to pay any amounts when due after providing notice of the suspension at least 30 days in advance.

8.3 **Termination for Cause.** When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Genesys shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

8.4 **Effects of Termination**.

8.4.1 **Parties' Obligations**. Upon the effective date of termination or expiration of this Agreement, all rights granted hereunder shall terminate and Customer must (i) stop using the Materials, and (ii) return or destroy from all computing and storage equipment all Supplier's, or its licensor, Genesys', Confidential Information in its possession or control, and all copies thereof, and verify such destruction or deletion by providing Supplier a statement signed by Customer's duly authorized representative. Within 30 days upon Customer's termination of this Agreement, a Services Order as provided in Section 8.3, Supplier will refund Customer a pro rata portion of any prepaid but unused fees corresponding to the remainder of the Subscription Term not rendered to the Customer. If Supplier terminates this Agreement or a Services Order, as provided in Section 8.3, Customer will pay Supplier, within 30 days upon such termination, any charges incurred up to the effective date of termination and any fees payable under the applicable Services Order(s) in effect at the time of termination.

8.4.2 **Retrieval of Customer Data**. If Customer requires additional time to retrieve its Customer Data from the Cloud Services beyond the date of termination, Customer may request, and Supplier will grant, a 30-day extension to the Subscription Term of the applicable Services Order; provided such request is made on or prior to the termination date. During the extended period, Customer will be charged for its usage of the Cloud Services. The Cloud Services will be terminated at the end of the extension period, unless otherwise agreed to by the parties.

8.4.3 **Survival of Terms.** Except as otherwise provided herein, neither party shall have further obligations under this Agreement, except that the parties shall remain bound by the obligations which, by their nature, are intended to survive termination.

9. CUSTOMER DATA

9.1 **Data Residency.** Customer Data will reside in the AWS Region selected by Customer throughout the Subscription Term of the relevant Services Order. Neither Supplier, nor its licensor, Genesys, will change the AWS Region without Customer's prior written consent. Customer Data may be accessed outside the selected AWS Region solely for the purposes of providing the Services, including maintenance, support and/or responding to a troubleshooting request, provided however, Supplier, or its licensor, Genesys, must always comply with its obligations under applicable privacy legislation. Customer Data will be processed in accordance with the terms of this Agreement and requirements of applicable law.

9.2 **Data Compliance.** Customer represents and warrants that it has obtained all the consents necessary for Supplier, and its licensor, Genesys, to collect, access, process, store, transmit, and otherwise use Customer Data in accordance with this Agreement. Customer acknowledges that Supplier, and its licensor, Genesys, has no control over the content of Customer Data, and Supplier, and its licensor, Genesys, expressly disclaim any duty to review or determine the legality, accuracy or completeness of Customer Data.

9.3 **Service Improvements.** Genesys may aggregate data and information related to the performance, operation and use of the Cloud Services to conduct statistical analyses, benchmarking, research, development, and other similar activities (**"Service Improvements"**). Genesys will not incorporate Customer Data in Service Improvements in a form that could identify Customer or Customer's customers and will use industry standard techniques to anonymize Customer Data prior to performing Service Improvements, unless otherwise consented to by Customer. Genesys retains all intellectual property rights in Service Improvements and may make them publicly available.

10. GENERAL

10.1 **Compliance with Applicable Laws.** Each party will comply with laws and regulations as applicable to such party, including all applicable anti-corruption and anti-bribery laws. Neither party will be responsible for the other party's compliance with the laws applicable to the other party. Customer represents and warrants that (i) neither Customer nor any of the authorized users within Customer's organization are on any government-issued list of restricted persons or entities, including the Consolidated List, 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 (ii) it will not export or re-export, directly or indirectly, any Materials or Confidential Information provided by Supplier or its licensor, Genesys, to any countries outside the United States except as permitted under the export control and sanctions laws and regulations of the United States and other countries that may prohibit or restrict access by certain persons or from certain countries or territories.

10.2 **Marketing.** Genesys may use Customer's name in marketing materials in reference to Customer's use of the Services, subject to Customer's prior written approval of the content to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71 .

10.3 **Assignment**. Neither party may assign its rights or obligations under this Agreement, either in whole or in part, except (i) with respect to a sale of substantially all of its assets, merger or change in the party's ownership in accordance with the provisions set forth at FAR 42.1204, except, in the case of Customer, to a competitor of Genesys, (ii) to an Affiliate, or (iii) with the prior written consent of the other party, which shall not be unreasonably withheld. The rights and liabilities of the parties hereto shall bind and inure to the benefit of their respective permitted successors and assigns.

10.4 **United States Government Usage.** The Materials are defined as "commercial items" under the Federal Acquisition Regulations and their use hereunder by the U.S. Government constitutes acknowledgment by the U.S. Government of Supplier's and its licensor, Genesys', proprietary rights therein and thereto. If the Materials are licensed by or on behalf of the U.S. Government or a state or local government in the United States, such government users shall obtain only the commercial license rights set forth in this Agreement, consistent with FAR 12.212.

10.5 **Subcontracting**. Supplier, or its licensor, Genesys, may subcontract certain services under this Agreement to third parties. Supplier, or its licensor, Genesys, shall be responsible for the performance of such subcontractors hereunder, as applicable.

10.6 **Force Majeure**. Except for payment obligations, in accordance with GSAR Clause 552.212-4(f), neither party will be responsible for any delay or failure to comply with its obligations under this Agreement resulting from acts beyond the reasonable control of such party, including acts of God, denial of service attacks, strikes, lockouts, riots, war, terrorism, pandemics, fire, communication line failures, power failures, earthquakes or other disasters, natural or man-made.

10.7 **Governing Law. Jurisdiction**. This Agreement shall be governed by the Federal laws of the United States. The UN Convention for the International Sale of Goods shall not apply to this Agreement. The prevailing party to any dispute shall be entitled to recover its cost of enforcing a claim.

10.8 **Third party beneficiaries**. To the extent permitted by applicable law, both parties acknowledge that Genesys and its Affiliates are intended third-party beneficiaries of this Agreement and that no other third- party rights are conferred by this Agreement.

10.9 **Notices**. All notices under this Agreement shall be in writing and deemed to have been given when (i) personally delivered, (ii) sent by registered mail, postage prepaid (which shall be deemed to have been received on the third business day following the date on which it is mailed), or (iii) sent overnight by a commercial overnight courier that provides a receipt (which shall be deemed to be received on the next business day after mailing).

10.10 **Waiver and Remedies**. No provision of this Agreement may be waived unless such waiver is in writing and signed by the party against which the waiver is to be effective. A party's failure to act with respect to a breach of this Agreement by the other party does not constitute a waiver of its rights with respect to subsequent or similar breaches. Except as otherwise provided herein, all remedies herein are cumulative, and the specification of a remedy will not preclude either party from pursuing other remedies available at law or in equity.

10.11 **Complete Agreement**. This Agreement constitutes the complete agreement between the parties and supersedes all prior agreements and representations, written or oral, concerning the subject matter hereof. Use of any purchase order or other document Customer provides in connection with this Agreement will be for administrative convenience only and all terms and conditions stated therein will be void and of no effect. Without prejudice to updates to terms in accordance with Section 2.4, this Agreement may not otherwise be modified or amended except in writing signed or executed by a duly authorized representative of each party. Except as expressly provided herein, each party acknowledges and agrees that it is not relying upon any other statements, representations, warranties, promises, assurances, the delivery of future functionality or features, or the like.

Security Policy for Genesys Cloud Services

These security terms for Cloud Services ("**Cloud Security Terms**") form part of agreement between Customer and Genesys for the supply of the Cloud Services ("**Master Agreement**"). These Cloud Security Terms set out the security and compliance posture related to the provision by Genesys of the Cloud Services that Customer has purchased from Genesys pursuant to the Master Agreement. These Cloud Security Terms are applicable to the extent that Genesys has access and control over Customer Data, as defined below. For avoidance of doubt, these Cloud Security Terms do not apply to applications purchased via the AppFoundry Marketplace (even if such application is created by Genesys) or to Genesys Professional Services.

1 Definitions

1.1 **Cloud Services** means Genesys-operated cloud offerings that are based on Genesys proprietary software deployed in a Genesys-managed Cloud Services Environment, and the support for such offerings.

1.2 **Cloud Services Environment** means the Genesys-controlled infrastructure, including equipment, servers and software, within Data Centers used to provide Cloud Services.

1.3 **Customer Data** means Customer's data that is inputted, or generated from Customer-inputted data, and stored in the Cloud Services. Customer Data does not include any anonymized data incorporated into Service Improvements pursuant to the Master Agreement.

1.4 **Data Center** means a data center where Genesys houses the Cloud Services Environment.

1.5 **Industry Standard** means generally accepted cloud information security practices as reflected in Genesys' policies and procedures.

1.6 **Malicious Code** means 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.

1.7 **Organisation/Org** means a dedicated Cloud Services instance. Each Org is assigned to a single AWS Cloud Services region and has a unique Org Name and Org ID.

1.8 **Security Incident** means a confirmed event resulting in the unauthorized use, deletion, modification, disclosure, or access to Customer Data.

1.9 **User** means an individual who: (i) is authorized by Customer and has been supplied a user identification and password(s) by Customer to access the Cloud Services on Customer's behalf, or (ii) a person licensed to use the Cloud Services for one or more roles (e.g. agent, supervisor, administrator).

2 General

2.1 **Shared Responsibility.** Security of Customer Data is a shared responsibility between Genesys and Customer, as set out in these Cloud Security Terms and at https://www.genesys.com/company/trust/resources.

2.2 **Security of the AWS Cloud Services.** Amazon Web Services is responsible for protecting the infrastructure that runs AWS services, including the Cloud Services, in the AWS Cloud. Oversight of AWS' security posture is managed in accordance with the agreement between AWS and Genesys. AWS-specific certifications are available at https://aws.amazon.com/compliance/programs. Security and compliance certifications and/or attestation reports for Data Centers must be obtained directly from AWS. AWS may require Customers to execute additional non-disclosure agreements. Third-party auditors also regularly test and verify the effectiveness of AWS security as part of AWS' internal compliance programs. Details on AWS data center specific security controls can be found here: https://aws.amazon.com/compliance/data-center/controls/.

2.3 **Security of the Cloud Services Platform**. Genesys is responsible for the security of the Cloud Services that run on the AWS cloud infrastructure. This includes the cloud-hosted application and related Cloud Services applications, including but not limited to Genesys Cloud User Client, Genesys Cloud Collaborate, Genesys Cloud Communicate.

2.4 **Security of Customer's Cloud Services Org.** The Customer is responsible for the security of its Cloud Services Org. This security is dependent on Org-specific configurations, and user access restrictions, both of which fall under the Customer's control.

3 Genesys Security Program

3.1 **Security Standards**. Genesys has implemented and will maintain an information security program designed to protect Customer Data processed in the Cloud Services that follows generally accepted system security principles embodied in the ISO 27001 standard, as appropriate to the nature and scope of the Cloud Services provided. For Genesys Cloud Commercial AWS regions, the Cloud Services will maintain, as a minimum, industry standard certifications such as SOC2 Type 2, ISO 27001, C5 and PCI DSS. The then-current list of certifications and attestations applicable to the Cloud Services can be found at https://www.genesys.com/company/trust/compliance.

3.2 **Security Awareness and Training**. Genesys has developed and will maintain an information security and awareness program that is delivered to all Genesys 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. Specifically, this includes annual compliance training on information security, privacy, HIPAA security & privacy, and PCI. Access to Genesys' code repository requires additional annual training in secure development.

4 **Policies and Procedures.** Genesys will maintain appropriate policies and procedures to support the information security program. Policies and procedures will be reviewed at least annually and updated as necessary with the aim of increasing the level of security protection for the Cloud Services. Customers can subscribe to updates to the Cloud Services Security Policy at this page - https://help.genesys.cloud/subscribe-to-policies/ S.

5 **Change Management.** The Cloud Services utilize a change management process based on ISO 27001 standards to ensure that all changes to the Cloud Services Environment are appropriately reviewed, tested, and approved.

6 **Data Storage and Backup.** Genesys will create backups of Customer Data. Customer Data will be stored in the same AWS Region as the Customer's Cloud Services Org and maintained using Server-Side Encryption (SSE). Backup data will not be stored on portable media. Customer Data backups are protected from unauthorized access and are encrypted.

7 **Anti-virus and Anti-malware.** Industry Standard anti-malware protection solutions are used to protect the infrastructure that supports the Cloud Services against threats such as Malicious Code. Genesys deploys File Integrity Management (FIM) solutions on all production systems, as well as robust monitoring of system access and command use.

8 **Vulnerability and Patch Management.** Genesys will maintain a vulnerability management program as per Genesys risk management process, that ensures compliance with Industry Standards. Genesys will assess all critical vulnerabilities to the Cloud Services Environment using industry standard CVSS and CVE scores or other similar approach for access/vector complexity, authentication, impact, integrity, and availability. If Genesys deems the resulting risk to be critical to Customer Data, Genesys will endeavour to patch or mitigate affected systems within three (3) working days. Certain stateful systems cannot be patched as quickly due to interdependencies and customer impact, but will be remediated as expeditiously as practicable. In normal operation OS patch management operations will be performed in 30 (thirty) days or less.

9 **Data Deletion and Destruction, Exit Plan.** Genesys will follow, and will ensure that its sub-processors will follow, Industry Standard processes to delete obsolete data and sanitize or destroy retired equipment that formerly held Customer Data. Customer Org related recording and call detail record retention policies are customer configurable. All other retention policies are managed by Genesys at platform level. Termination of the Cloud Services for Customer will be subject to the Exit Plan in Exhibit A.

10 Penetration Testing.

10.1 **Independent 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. Test results will be made available to Customer upon written request and will be subject to non-disclosure and confidentiality agreements.

10.2 **Customer Testing.** Customers have the option to run a penetration test in conjunction with Genesys Security teams within agreed parameters. This service is chargeable at Genesys' then-current rates. Customer will be required to enter into a Services Order for two Test Orgs and a Statement of Work for related professional services support. This service is available once per year. Customer will not perform any type of penetration testing, vulnerability assessment, or denial of service attack on the Cloud Services production, test, or development environments save as set out above.

11 Product Architecture Security

11.1 **Logical Separation Controls**. The Cloud Services are a multi-tenanted Software as a Service (SaaS) platform. As such, customers on the platform share resources such as server instances, services, data storage locations and databases. Genesys will employ effective logical separation controls based on Industry Standards to ensure that Customer Data is logically separated from other customer data within the Cloud Services Environment. More detail can be found here: https://help.genesys.cloud/articles/multitenant-security/

11.2 **Firewall Services**. Genesys uses Security Groups and appropriate firewall services to protect the Cloud Services Environment. Genesys maintains granular ingress and egress rules, and changes must be approved through Genesys' change management system.

11.3 **Intrusion Detection System.** Genesys has implemented intrusion detection across the Cloud Services that meets PCI DSS requirements.

11.4 **No Wireless Networks**. Genesys will not use wireless networks within the Cloud Services.

11.5 **Data Connections between Customer and the Cloud Services Environment**. All connections to browsers, mobile apps, and other components are secured via Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS v1.2 or higher) over public Internet.

11.6 **Data Connections between the Cloud Services Environment and Third Parties.** Transmission or exchange of Customer Data with Customer and any Genesys vendors will be conducted using secure methods (e.g. TLS 1.2 or higher).

11.7 **Encryption Protection**.

11.7.1 **Encryption Methods.** The Cloud Services use Industry Standard encryption methods to uphold confidentiality, integrity and availability of data being stored, processed and transmitted. The Cloud Services provide

a. at rest and in transit encryption of all processed Customer Data;

b. at rest encryption, which is AES 256-based meeting FIPS 197 standard, using encryption keys to which neither AWS and its subcontractors nor Genesys' subcontractors have access; and

c. in transit encryption, which is TLS 1.2 or higher using encryption keys to which neither AWS and its subcontractors nor Genesys' subcontractors have access.

11.7.2 **Recording Encryption**. The Cloud Services encrypt, as standard, call recordings for voice and digital communications with customer specific keys generated by Genesys but rotation can be managed by Customer. Customer may elect to implement customer-owned encryption keys for recordings, allowing Customer to store and manage its keys outside the Cloud Services. To the extent required by applicable law or Customer's policies, the Customer is responsible for the content of recordings and ensuring that PCI Data is not recorded, using Secure Pause or other tools made available by Genesys.

11.8 **Logging and Monitoring**. Genesys will log security events for the Cloud Services. Genesys will continuously monitor and investigate events that may indicate a Security Incident for the Cloud Services. Platform-related event records will be retained for at least one year. Audit log data related to Customer's Org is available to customers via the Cloud Services UI (https://help.genesys.cloud/articles/about-the-audit-log-viewer/) or the Cloud Services REST based API's or real-time stream (https://help.genesys.cloud/articles/about-the-amazon-eventbridge-integration/). Genesys Platform security logs are not available to customers.

12 Access Control

12.1 **Access Control.** Genesys will implement appropriate tools for access controls to ensure that only authorized Users have access to Customer Data within the Cloud Services Environment.

12.2 **Customer's User Access**.

12.2.1 **Usernames and Passwords**. Customer is solely responsible for managing User access controls within Customer's Org. The application password requirements are configurable by Customer. Native Multi-Factor Authentication (MFA) is available as part of the Cloud Services and is configurable by Customer. Password Parameters that can be set include minimum length, minimum letters, minimum numerals, minimum special characters, password expiration, and minimum age. Customer defines usernames and roles in a granular access permissions model. 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 wilful action or inaction, Customer is entirely responsible for all use of the Cloud Services through Customer's Org, whether or not authorized by Customer, and all charges resulting from such use.

12.2.2 **Single Sign On**. Customers can elect to integrate with a customer supplied Single Sign On (SSO) provider for authentication and can use Cross-domain Identity Management (SCIM) for user management. More detail on SCIM is available here: https://help.genesys.cloud/articles/about-genesys-cloud-scim-identity-management/ and on SSO here: https://help.genesys.cloud/articles/about-single-sign-on-sso/.

12.3 **Genesys' User Access.** Genesys will follow strict protocol and authorisation flows to create individual user accounts for each of Genesys' employees that have a business need to access Customer Data or Customer's systems within the Cloud Services Environment. The following protocol will be followed regarding Genesys' user account management:

12.3.1 **Accounts**. Genesys user accounts are requested by the relevant employee and authorized by Genesys management;

12.3.2 **VPN**. Genesys employees, who are approved to access the Cloud Services Environment use a client-to-site Virtual Private Network (VPN) for entry into the Cloud Services AWS Virtual Private Cloud (VPC) and they require multi-factor authentication;

12.3.3 **Password**. Genesys user passwords expire every ninety (90) days;

12.3.4 **Time-outs**. Session time-outs are systematically enforced;

12.3.5 **Termination**. Genesys user accounts are promptly disabled (within one working day) upon employee termination or role transfer that eliminates a valid business need for access;

12.3.6 **Endpoints**. Genesys users can only access the Cloud Services Environment from Genesys-managed endpoints. Genesys-managed endpoints have hard drive encryption enabled;

12.3.7 **Review**. Genesys employee accounts to the Cloud Services Environment are reviewed at least every 60 days.

13 Business Continuity and Disaster Recovery

13.1 **Business Continuity**.

13.1.1 **Availability Zones.** The Cloud Services are deployed and configured in a load balanced active/active/active design and are deployed across at least three AWS Availability Zones ("AZs") within a single region to provide high availability and performance of the Cloud Services. The Cloud Services are physically separated from Genesys' corporate network environment so that a disruption event involving the corporate environment does not impact the availability of the Cloud Services.

13.1.2 **Replication**. Using synchronous replication, Cloud Services data is automatically updated in multiple AZs. The Cloud Services use load balancers to route internal and external traffic to available application components. Load balancers are clusters of servers that load balance HTTP requests across multiple AZs. When the load balancer detects that a Cloud Services component is either at capacity or has failed, it routes traffic to other instances automatically to compensate. Both the Cloud Services public APIs and application components are fronted by load balancers.

13.1.3 **Regions.** List of Cloud Services regions can be found on https://www.genesys.com/cloud-platform/global-availability. Highly available architecture is explained under this link https://help.genesys.cloud/articles/about-architecture-and-technology/

13.2 **Disaster Recovery**. For the Cloud Services, disaster recovery (DR) tests are performed at least annually. Backup data is not stored off-site or on portable media. Genesys creates backups of Customer Data according to documented backup procedures. Customer Data is stored and maintained solely in Amazon AWS S3 with SSE in the same AWS region where Customer Data resides.

13.3 **Business Continuity and Disaster Recovery Plans.**

13.3.1 **Corporate Business Continuity Plan.** 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.

13.3.2 **Cloud Services Business Continuity Plan.** Genesys will maintain a Cloud Services business continuity plan designed to assure high availability with a target Recovery Time Objective (RTO) of zero and Recovery Point Objective (RPO) of zero.

13.3.3 **Testing.** The Cloud Services Business Continuity and Disaster Recovery Plans, annual testing of restores and BC/DR are audited annually as part of compliance audits (SOC 2 Type II, ISO 27001/27017/27018, PCI-DSS, HIPAA & HITRUST, etc.).

13.4 **Customer's Responsibility.** Customer is responsible for building and maintaining business continuity and disaster recovery plans for its operations, connectivity to the Cloud Services and other third-party services.

14 Security Incident Response

14.1 **Security Incident Response Program**. Genesys will maintain a Security Incident response program based on Industry Standards designed to identify and respond to Security Incidents involving Customer Data. The program will be reviewed, tested and, if necessary, updated on at least an annual basis.

14.2 **Notification**. In the event of a Security Incident or other security event requiring notification under applicable law, Genesys will notify Customer within twenty-four (24) hours and will reasonably cooperate so that Customer can make any required notifications relating to such event, unless Genesys specifically requested by law enforcement or a court order not to do so.

14.3 **Notification Details**. Genesys will provide the following details regarding any Security Incidents to Customer: (i) date on which the Security Incident was identified and confirmed; (ii) the nature and impact of the Security Incident; (iii) actions Genesys has already taken; (iv) corrective measures planned to be taken; and (v) evaluation of alternative measures and next steps.

14.4 **Ongoing Communication**. Genesys will continue providing status updates to Customer regarding the resolution of the Security Incident and continually work in good faith to correct the Security Incident and prevent future such Security Incidents. Genesys will cooperate, as reasonably requested by Customer, to further investigate and resolve the Security Incident.

15 Use of the Cloud Services

15.1 **VoIP Services Lines**. Customer shall maintain strict security over all VoIP Services lines.

15.2 **Recordings**. Customer acknowledges that use of recordings is within Customer's sole 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 configuring and using the Cloud Services accordingly; and (ii) Customer shall ensure that recordings shall be made only for purposes required by and/or in compliance with, all applicable laws. Customer will ensure that recordings will not knowingly include any bank account number, credit card number, authentication code, social security number or personal data, except as permitted by all applicable laws.

16 Audit of Genesys Security Compliance

16.1 **Customer Audit**. Provided that Customer has demonstrated that it has a reasonable belief that Genesys is not in compliance with the security standards in Section 3.1 above and subject to Genesys' reasonable confidentiality and information security policies, Customer or a qualified third party chosen by Customer shall have the right, upon at least thirty (30) days' written notice, to perform a remote audit of Genesys' compliance with the terms of these Cloud Security Terms, limited to review of Genesys certifications and attestations, policies, interviews of key personnel, and the completion of a security assessment questionnaire provided by Customer.

16.2 **Audit Requirements.** Customer may undertake an audit without reasonable belief described in 16.1, provided that:

a. The audit is performed during normal business hours,

b. Genesys will invoice Customer a fee for Genesys' costs incurred (including internal time spent) in connection with any Customer audit, whether the audit was performed remotely or on-site,

c. The scope and price of the audit will be agreed upon by the parties in a Statement of Work,

d. Customer agrees that such audit will not include the right to on-site inspections or audits of any of Genesys' subcontractors, including Genesys' third-party hosting facilities and equipment,

e. The audit will not violate Genesys' obligations of confidentiality to other customers or partners, or reveal Genesys' intellectual property, and

f. Any assessment performed pursuant to this section shall not interfere with the normal conduct of Genesys' business.

16.3 **Cooperation**. Genesys shall cooperate with Customer on any reasonable requests made by Customer during such assessments.

Exhibit A

EXIT PLAN or Off-Boarding Plan

The following details the process of offboarding a customer from the Cloud Services:

1. **Initiation**. The Exit Plan process will be initiated upon expiration or receipt of formal notice of termination of contract by either party, as detailed in the Master Agreement.

2. **Exit Plan and Data Transfer Approach for the Cloud Services.** Customer will be able to use the Cloud Services APIs to retrieve the following customer data as stated in the Master Agreement:

    a. **Customer Data (Reporting Metrics) Handover:** Customer data can be exported during or at contract termination by using Genesys' APIs on this link: https://developer.genesys.cloud/api/rest/v2/analytics/data_integration_guide.html. In the event that Customer requires additional time to export Customer Data beyond the date of contract termination or expiry, Customer shall request a service extension period in accordance with the Master Agreement.

    b. **Customer Data (Recordings) Handover:** Recordings can be exported during the contract term or at the contract termination by using Genesys' Recording Export APIs. For further information please refer to this link below: https://developer.genesys.cloud/api/tutorials/recordings-bulk-actions.

3. **Extensions.** In the event that Customer requires additional time to export recordings beyond the date of contract termination or expiry, Customer shall request an extension of the Subscription Term before the termination or expiry date, as set out in the Master Agreement.

4. **Professional Services.** Customers can use the Cloud Services API to build their own applications or engage with Genesys professional services for further assistance.

5. **Troubleshooting.** Troubleshooting and other platform logs are not provided or returned. Genesys is required to keep such logs for a minimum of one (1) year as part of its compliance program.

6. **Third Party Applications.** Any Third-party applications (for example, AppFoundry Apps) are outside the scope of the Cloud Services exit/offboarding plan.