ADDENDUM TO THE GENESYS CLOUD SERVICES AGREEMENT
For the Genesys Cloud Analytics Add-on (A3S)

1. PREAMBLE

1.1. This Addendum to the Genesys Cloud Services Agreement (“Addendum”) incorporates by reference the Genesys Cloud Services Agreement (“**Agreement**”) between Customer and Genesys and, collectively, these agreements compose the terms and conditions for the Customer’s purchase of Genesys Cloud Analytics Add-on Services (“**A3S**”).

1.2. Any capitalized terms used in this Addendum which are not otherwise defined herein are as defined in the Agreement. For the avoidance of doubt and unless otherwise specified in this Addendum, any reference to “Genesys Cloud Services”, “Services” and “Cloud Services” in the body of the Agreement shall be taken to include A3S, and any references to “Documentation” shall include (where appropriate) “A3S Documentation” (as defined below).

1.3. Except as amended herein, all other terms of the Agreement shall remain in full force and effect. In relation to A3S only, the order of precedence of the documents forming the Agreement is as follows: 1) this A3S Addendum, 2) Agreement, 3) Services Order.

2. DEFINITIONS

The following definitions are added to the Agreement for the purposes of A3S:

A3S: a Genesys software-as-a-service offering that provides automated data integration, a cloud-scale analytical data warehouse (Historical), real-time event bridge data delivered in a dashboard tool (Real-time), and preconfigured reporting and analytics dashboards, as described in the then-current A3S Documentation, but specifically excluding related Professional Services.

A3S Documentation: the then-current technical instructions and product description for A3S, as updated from time to time, located at https://help.mypurecloud.com/articles/genesys-cloud-add-ons/ or such other website as Genesys may notify to Customer from time to time.

User(s): individuals who are authorized by the Customer to use A3S, and who have been supplied user identifications and passwords by the Customer (or by Genesys at the Customer’s request). Users consist of any employees of the Customer or its Affiliates and any independent contractors of the Customer or its Affiliates who access A3S on Customer’s behalf.

3. ADDITIONAL TERMS FOR A3S

For the purposes of A3S only, the following clauses are inserted into the Agreement:

2.1A **A3S Access Rights.** Subject to the terms and conditions of this Agreement, Genesys grants Customer a non-exclusive, non-transferable, revocable, worldwide right to authorize Users to use and access A3S and the A3S Documentation solely for Customer’s internal business purposes during the Subscription Term. Customer has no right to receive a copy of the object code or source code versions of A3S.

2.3A **A3S Support.** Genesys will provide support for A3S in accordance with Genesys Custom Application Support, as described in Appendix A to this Addendum, which supersedes the Genesys Cloud Service Level Agreement located at https://help.mypurecloud.com/articles/service-level-agreements/.

2.3B **A3S Security**. For purposes of A3S only, the security terms located at https://help.mypurecloud.com/articles/genesys-cloud-security-policy/ (“Security Policy”) are hereby modified as set out in Appendix B to this Addendum. In the event of any conflict or inconsistency between the Security Policy and Appendix B, the terms in Appendix B will prevail.

2.4A Genesys reserves the right to make updates to the support and/or security terms for the A3S during the Subscription Term. If, however, such a change results in the material degradation of the level of support for A3S or the level of protection of Customer Data hosted in A3S, and no workaround has been provided by Genesys, then Customer may terminate its subscription to A3S by providing Genesys with written notice within 30 days from the date of notification of such change.

APPENDIX A
Genesys Custom Application Support

The Genesys Custom Application Support for Cloud ("**Cloud CAS**") is a break/fix support service that provides support plans with problem identification and resolution for A3S in the context of a broader Genesys solution.

1. Genesys will provide the following services during the Subscription Term outlined in the Services Order:

1.1. Problem identification and resolution with break/fix support services, documentation updates, and new versions, as available, for A3S.

1.2. Remote telephone support with Web and/or email assistance according to the Support Response Targets and hours of operation as stated in the Custom Application Support Program Guide for Cloud ("**Support Guide**") available at https://ps.genesys.oncaas.com/Genesys_Custom_Application_Support_Program_Guide_Cloud_v1.0.4.doc, which is incorporated into this Appendix A.

1.3. Upgrades and patches for A3S to ensure continuous operation.

2. Customer shall appoint at least two (2) employees to initiate and manage support inquiries ("**Designated Contacts**"). Designated Contacts shall have competent knowledge of A3S. Only Customer's Designated Contacts are allowed to submit support requests. Genesys shall be entitled to charge reasonable additional fees for services provided beyond the scope of its support obligations set forth herein.

3. Customer's access and use of support are subject to the terms of the Support Guide. Genesys reserves the right to update support case management processes as needed and may elect to post an announcement on the Customer Care portal. Customer will submit requests for support subject to the processes set forth in the Support Guide. Prior to reporting an issue, Customer shall investigate the issue and make reasonable use of the self-help guides and information posted on the Customer Care Portal. Customer Designated Contacts must be knowledgeable and have access to information to facilitate resolution of reported issues. Genesys is not responsible for resolving issues that cannot be reproduced in a controlled test environment. All issues reported by Customer via Genesys Customer Care are tracked in the Customer Care Case Management Tool and assigned a case number for tracking purposes. Customer shall include the case number in all communications regarding a reported issue.

4. Cloud CAS Exclusions

4.1. Genesys shall not provide Cloud CAS relating to A3S defects arising out of:

4.1.1. Any alterations of or additions to A3S by parties other than Genesys or at the written direction of Genesys;

4.1.2. Use of A3S not in accordance with the provided documentation;

4.1.3. Changes to the operating environment which adversely affect A3S;

4.1.4. Modifications to the access criteria, security, customer interfaces, or peripheral systems to be used by A3S;

4.1.5. Accident, negligence, or misuse of A3S;

4.1.6. Issues caused by Customer owned non-Genesys or third-party applications or Customer maintained infrastructure (e.g., network, Agent Desktop, Customer relationship management (CRM), Web Servers, Databases, Stored Procedures, Mainframes, etc.); and

4.1.7. Interconnection of A3S with software not supported by Genesys.

4.2. **Resolution of Non-Genesys Problems**. Genesys will investigate and diagnose all cases opened related to A3S. Genesys will use commercially reasonable efforts to provide resolution to defects found within A3S service code. Upon receipt of a support case from Customer, Genesys will initially perform problem determination. After this problem determination period, should Genesys determine there is significant likelihood that a reported problem is caused by factors outside of Genesys' control, including but not limited to Customer's firewall, database, network, telecommunications equipment, host computers or applications ("**Non-Genesys Problem**"), Genesys will notify Customer thereof as soon as Genesys is aware of such Non-Genesys Problem. Customer will have the option to assume responsibility for further problem diagnosis and resolution or to approve continued investigation and work on resolution of the Non-Genesys Problem via a new Genesys Professional Services Statement of Work. Services will be provided during normal business hours and at the then-current applicable Genesys Professional Services hourly rate.

5. Customer Responsibilities

5.1. Customer will ensure the participation of key technical and business personnel so that requirements can be defined without delay. Customer will provide access to its technical and functional subject matter experts on a timely basis to work in a collaborative manner with Genesys consulting resources.

5.2. Customer will provide relevant supporting documentation, as requested by the Genesys Care personnel. This may include any current and planned environment configuration, network topology schematics, and system logs.

5.3. Customer will be responsible for network, switch, system, and database administration during the Subscription Term of the Cloud CAS.

5.4. Customer will ensure that all servers, operating systems, and LAN/WAN connectivity are operational, and access made available throughout the Subscription Term.

6. Additional Terms

6.1. All Cloud CAS services will be provided remotely.

6.2. Travel and living expenses are not included in the annual fees. If both Customer and Genesys determine that onsite support is necessary, any travel and living expenses will be agreed with Customer prior to incurring the expenses and Customer will issue a valid Purchase Order equal to the estimate. Travel and living expenses incurred by Genesys will be billed monthly at actual cost.

6.3. To minimize communication discrepancies, any and all official communications, written, spoken, electronic, or otherwise, in support of the delivery of the services outlined herein must be in the English language.

APPENDIX B

Modifications to Genesys Cloud Security Policy for A3S

1. Security Attestations

A3S security and operational controls are SOC 2 Type I, ISO 27001, and HIPAA.

2. Data Storage and Backup

Customer Data will be stored in the AWS Region selected by Customer for its A3S deployment. This may not be in the same AWS Region as Customer's Genesys Cloud org. A3S backup data will not be stored on portable media. A3S Customer Data backups are protected from unauthorized access and are encrypted.

3. Exit Plan

Customer Data can be exported directly from A3S using native file export functionality.

4. Vulnerability and Patch Management

Genesys will assess all critical vulnerabilities to the A3S AWS production environment 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 fourteen calendar days.

5. Encryption Protection

1. Encryption Methods

A3S uses Industry Standard encryption methods to uphold confidentiality, integrity and availability of data being stored, processed, and transmitted, as follows:

- At rest and in transit encryption of all Customer Data processed in A3S
- At rest encryption is AES 256-based
- In transit encryption is TLS 1.2 or higher

2. Customer's User Access

1. Customer is solely responsible for managing User access controls within Customer's A3S instance. The application password requirements are configurable. MFA is available. 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 A3S through Customer's Org, whether or not authorized by Customer, and all charges resulting from such use.

2. 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.

3. Genesys' User Access

1. Genesys employees who are approved to access the A3S Environment require multi-factor authentication, but the VPN, VDI, and direct access to product prohibitions and controls in Genesys Cloud do not extend to the A3S environment.
2. Genesys employee account access to the A3S environment is reviewed at least every 90 days.

6. Business Continuity

A3S is deployed and configured in a load balanced active/active design and are deployed across at least two, and sometimes three AWS Availability Zones ("AZs") within a single AWS Region to provide high availability and performance of A3S. Genesys Cloud is always deployed across three AWS AZs.