# Genesys Data Processing Addendum

Controller to Processor Standard Contractual Clauses

This Data Processing Addendum ("**DPA**") is entered into by and between. Genesys Cloud Services B.V. and Customer, below defined, as of the date last executed by the Parties. This Addendum adds to, and is governed by, the Master Agreement (as further defined), and takes the form of the *Standard Contractual Clauses* (SCC) as issued by Decision (EU) 2021/915.[1]

These SCC were drafted to oversee the relationship between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

For this Addendum to be effective, it is required that all contracting Parties reside within the European Economic Area.

| **Genesys** | **Customer** |
|---|---|
| Genesys Cloud Services B.V. | [Customer] |
| (the *"Processor"*) | (the *"Controller"*) |
| Prins Bernhardplein 200, 1097 JB Amsterdam, The Netherlands | [Customer Address] |
| DataPrivacy@genesys.com | [Customer email] |
| [Genesys Signature] | [Customer Signature] |
| [Genesys Signatory]<br>Authorized Representative's Name | [Customer Signatory]<br>Authorized Representative's Name |
| [Genesys Signatory Title]<br>Title | [Customer Signatory Title]<br>Title |
| [Month Day, Year] | [Month Day, Year] |

[1] Translations of such Standard Contractual Clauses to other languages are available in the following link: https://eur-lex.europa.eu/legal-content/DE-EN/TXT/?from=de&uri=CELEX%3A32021D0915

## SECTION I

*Clause 1*

### *Purpose and scope*

(a)The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

(b)The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e)These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f)These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

*Clause 2*

### *Invariability of the Clauses*

(a)The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b)This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

*Clause 3*

### *Interpretation*

(a)Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b)These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c)These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

*Clause 4*

### *Hierarchy*

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 5*

### *Docking clause*

(a)Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b)Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c)The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

## SECTION II

**OBLIGATIONS OF THE PARTIES**

***Clause 6***

***Description of processing(s)***

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

***Clause 7***

***Obligations of the Parties***

**7.1. Instructions**

(a)The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b)The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

**7.2. Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

**7.3. Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

**7.4. Security of processing**

(a)The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b)The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**7.5. Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

**7.6. Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b)The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c)The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d)The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e)The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

**7.7. Use of sub-processors**

(a)GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b)Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c)At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d)The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e)The processor shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**7.8. International transfers**

(a)Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b)The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

***Clause 8***

***Assistance to the controller***

(a)The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b)The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c)In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1)the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2)the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3)the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679/.

(d)The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

***Clause 9***

*Notification of personal data breach*

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

### 9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a)in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b)in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679/:

(1)the nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3)the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c)in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

### 9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a)a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c)its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

## SECTION III

## FINAL PROVISIONS

### *Clause 10*

### *Non-compliance with the Clauses and termination*

(a)Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b)The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1)the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2)the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3)the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c)The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d)Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

---

## ANNEX I

### List of parties

**Controller(s):** [Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer*]*

1. Name:

   Address:

   Contact person's name, position and contact details:

   Signature and accession date:

2.

**(s):** [Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer*]*

1. Name: Genesys Cloud Services B.V./Genesys Europe B.V.

   Address: Prins Bernhardplein 200, 1097 JB Amsterdam, The Netherlands

   Contact person's name, position and contact details: William Dummett, Chief Privacy Officer. Shahzad Ahmad,

   Data Privacy Officer. DataPrivacy@genesys.com

   Signature and accession date:

2.

## ANNEX II

### Description of the processing

**Categories of data subjects whose personal data is processed**

The Customer Data is processed to the extent determined by Controller Instructions, and may include but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Services

**Categories of personal data processed**

The Customer Data is processed to the extent of which is determined by Controller Instructions, and may include but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data
- Other categories of data as customized by the Data Controller

**Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

N/A

**Nature of the processing**

Genesys will process Customer Data pursuant to the Master Agreement, as further specified in the Documentation, and as further instructed by Controller Instructions.

**Purpose(s) for which the personal data is processed on behalf of the controller**

Genesys will process Customer Data pursuant to the Master Agreement, as further specified in the Documentation, and as further determined by Controller Instructions.

**Duration of the processing**

Subject to the DPA, Genesys will process Customer Data for the duration of the Master Agreement, unless otherwise agreed upon in writing.

**For processing by (sub-) processors, also specify subject matter, nature and duration of the processing**

Genesys Cloud services are hosted by third party data center providers. Premise services operate on systems controlled and operated by the Customer. Genesys may share personal data with any affiliated Genesys entities under common control with Genesys for (i) troubleshooting and (ii) support.

Genesys may utilize sub-processors, depending on what services, features, and functionality the customer utilizes. Additional sub-processors may be selected by Customer in a customized environment, and if so, such sub-processor will be listed in a Statement of Work or Order Form.

Customer acknowledges that signature of such Statement of Work or Order Form constitutes written consent for use of such sub-processor named therein. Note that third party integrations, such as AppFoundry, **require a direct relationship** between the third party and the Customer.

The sub-processors listed at the following website (along with its subsidiary companies) may be utilized, depending on what services and functionality is selected by the Customer. Customer acknowledges that changes to this website shall constitute notice of changes to sub-processors in accordance with section 7.7 Use of Sub-processors of this DPA.

https://help.mypurecloud.com/articles/genesys-subprocessors/

## ANNEX III

### Technical and organisational measures including technical and organisational measures to ensure the security of the data

Genesys provides a number of solutions and configurations for its platforms. The following TOMs apply to the offer specified below. Anything not listed below are covered by the Genesys Minimum Security Controls. Note that any third-party product that is resold by Genesys or integrates with Genesys will have security controls specific to that third party.

| Offer | Applicable TOMs |
|---|---|
| MultiCloud CX (fka Engage Cloud) | Cloud Services |
| MultiCloud Private Edition (fka Engage Premise) | Premise Support |
| PureConnect Cloud | PureConnect Cloud |
| PureConnect Premise | Premise Support |
| Genesys Cloud CX | Cloud Services |
| Predictive Engagement | Cloud Services |
| PureConnect Premise WhatsApp Hybrid<br>PureConnect Premise with Cobrowsing | Premise Support for the PureConnect services, and Cloud Services for the Cobrowsing/WhatsApp integration |
| Genesys Hub | Genesys Minimum Security Controls |
| WEM 2.0 | Cloud Services |
| Genesys DX (fka Bold360) | Genesys DX |

## Genesys Minimum Security Controls

This Appendix describes the minimum-security requirements generally applicable to Customer's use of Genesys Services. Additional controls for specific services or modules can be found in the applicable Agreement. Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Therefore, Processor will use necessary reasonable technical, organizational and security measures designed to protect Personal Data of Customer in possession of Processor or otherwise processed by Processor against unauthorized access, alteration, disclosure or destruction, as further described in this Appendix:

### 1. <u>Security Program</u>

We have implemented and will maintain an information security program that follows generally accepted system security principles embodied in the SOC-2 standard designed to protect the Customer Data as appropriate to the nature and scope of the Services provided. The information security program includes at least the following elements:

#### a. Security Awareness and Training

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

#### b. Policies and Procedures

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

#### c. Malware Prevention

We use industry standard practices to avoid the inclusion of any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan Horses) in applications running within Genesys services.

### 2. <u>Network Security</u>

Genesys will employ effective network security controls based on industry standards to ensure that Customer Data is protected.

### 3. <u>User Access Control</u>

Genesys will implement appropriate access controls to ensure only authorized users have access to Customer Data.

### 4. <u>Business Continuity and Disaster Recovery</u>

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.

### 5. <u>Security Incident Response</u>

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

## Cloud Services

These security terms for Cloud Services ("Cloud Security Terms") are incorporated by this reference into this Agreement with Genesys and describe the contractual requirements for information security provided by Genesys to Customer related to the provision of Cloud Services that Customer has licensed from Genesys pursuant to this Agreement. These terms are applicable to the extent that Genesys has access and control over Customer Data.

### 1. Security Program

**1.1.** Security Standards. 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 Customer Data, as appropriate to the nature and scope of the Cloud Services provided.

**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. Specifically, with regard to Customer Data access, this includes annual compliance, information security, privacy, HIPAA security & privacy, and PCI training. Access to Genesys' code repository requires additional annual training in secure development.

**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 the Cloud Services environment are appropriately reviewed, tested, and approved.

**1.5.** Data Storage and Backup. Genesys will create backups of critical Customer Data. Customer Data will be stored and maintained using cloud provider-based Server-Side Encryption (SSE). Backup data will not be stored on portable media. Customer Data backups will be protected from unauthorized access.

**1.6.** Anti-virus and Anti-malware. Industry Standard anti-virus and anti-malware protection solutions are used on systems commonly affected by malware to protect the infrastructure that supports the Cloud Services against malicious software, such as Trojan horses, viruses, and worms. Genesys deploys File Integrity Management (FIM) solutions on all production systems, as well as robust monitoring of system access and command use. Cloud Services server instances are primarily Linux, which is a system not commonly affected by malware. Where Windows-based server instances are used, Industry Standard anti-malware software is deployed.

**1.7.** Vulnerability and Patch Management. Genesys will maintain a vulnerability management program that ensures compliance with Industry Standards. Genesys will assess all critical vulnerabilities to the Cloud Services production environment for access/vector complexity, authentication, impact, integrity, and availability. If the resulting risk is deemed to be "Critical" to Customer Data by Genesys, Genesys will endeavour to patch or mitigate affected systems within 7 working days. Certain stateful systems cannot be patched as quickly due to interdependencies and customer impact but will be remediated as expeditiously as practicable.

**1.8.** Data Deletion and Destruction. Genesys will, and will ensure that subprocessors will, follow Industry Standard processes to delete obsolete data and sanitize or destroy retired equipment that formerly held Customer Data. Recording retention policies are determined by Customer and can be used as part of a routine deletion process for recorded interactions. For instance, a recording retention policy can be created to delete conversations that occurred within a range of dates. All deletion within the Cloud Services is a simple deletion. Secure data deletion is not applicable in a virtual disk environment.

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

### 2. Product Architecture Security

**2.1.** Logical Separation Controls. Genesys will employ effective logical separation controls based on Industry Standards to ensure that Customer Data is logically separated from other customer data within Cloud Services environment.

**2.2.** Firewall Services. Genesys uses firewall services to protect the Cloud Services infrastructure. Genesys maintains granular ingress and egress rules, and changes must be approved through Genesys' change management system. Rulesets are reviewed semi-annually.

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

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

**2.5.** 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) over public Internet (note some Cloud Voice telephony cannot be due to carrier limitations).

**2.6.** 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, HTTPS, SFTP).

**2.7.** Encrypted Recordings. Genesys encrypts call recordings and chat sessions. Customer may elect to implement Local Key Encryption and maintain Customer's own keys for voice and screen recordings. To the extent required by applicable law or Customer's policies, Customer is responsible for the content of recordings and ensuring PCI Sensitive Authentication Data is not recorded, using applicable security features or other tools made available by Genesys.

**2.8.** Encryption Protection. Genesys uses Industry Standard methods to support encryption, with AES and TLS 1.2. Digital Recording encryption is addressed in Sections 2.7 and 7.6.

**2.9.** Logging and Monitoring. Genesys will log security events from the operating perspective for all infrastructure providing the Cloud Services to Customer. Genesys will monitor and investigate events that may indicate a Security Incident or problem. Event records will be retained at least one year. Limited audit data is accessible to customers via the User Interface (UI) and Application Programming Interface (API).

## 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 Cloud Services environment.

**3.2.** Customer's User Access. Customer is responsible for managing User access controls within the application. The Cloud Services application password requirements are configurable by Customer for minimum length, minimum letters, minimum numerals, minimum special characters, password expiration, and minimum age. Genesys has a lockout period after several invalid attempts. Most Users experience a lockout period after 5 bad attempts, but Customer can automatically try again in 5 minutes. These settings are not configurable. 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 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 Cloud Services.

**3.3.** Genesys' User Access. Genesys will 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 guidelines will be followed regarding Genesys' user account management:

**3.3.1.** User accounts are requested and authorized by Genesys management.

**3.3.2.** Strong password controls are systematically enforced.

**3.3.3.** Connections are required to be made via secure VPN using strong passwords that expire every ninety (90) days and multi-factor authentication.

**3.3.4.** Session time-outs are systematically enforced.

**3.3.5.** User accounts are promptly disabled upon employee termination or role transfer that eliminates a valid business need for access.

## 4. Business Continuity and Disaster recovery

**4.1.** Disruption Protection. The Cloud Services will be deployed and configured in a high-availability design and will be deployed across separate Data Centers to provide optimal availability of the Cloud Services. The Cloud Services environment is 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.

**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 Cloud Services platforms take advantage of the distributed nature of the infrastructure to enable full multi-site disaster recovery by operating in multiple availability zones ("AZ's"); distinct locations that are engineered to be insulated from each other. Independent application stacks are run in multiple AZ's. In the event of the loss of a single AZ or data center, the remaining Cloud Services remain operational and are designed to auto-scale to replace the lost system capacity.

## 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 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 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.

**5.3.** Notification Details. Genesys will provide the following details regarding any Security Incidents to Customer: (i) date that 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 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 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.

**6. Data Center Protections.** Genesys contracts with Data Centers for Platform as a Service (PaaS). Security and compliance certifications and/or attestation reports for Data Centers must be obtained directly from the Data Center. Data Center may require Customer to execute additional non-disclosure agreements.

**7. Use of the Cloud Services**

**7.1.** Use Restrictions. Customer will not, and will not permit or authorize others to, use the Cloud Services for any of the following: (i) to violate applicable law; (ii) to transmit malicious code; (iii) to transmit 911 or any emergency services (or reconfigure to support or provide such use); (iv) to interfere with, unreasonably burden, or disrupt the integrity or performance of the Cloud Services or third-party data contained therein; (v) to attempt to gain unauthorized access to systems or networks; or (vi) to provide the Cloud Services to non-User third parties, including, by resale, license, lend or lease.

**7.2.** Customer Testing Restrictions. 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.

**7.3.** Prohibited Use. Customer will use commercially reasonable efforts to prevent and/or block any prohibited use by Users.

**7.4.** Customer Safeguards. Customer will maintain a reasonable and appropriate administrative, physical, and technical level of security regarding its account ID, password, antivirus and firewall protections, and connectivity with the Cloud Services.

**7.5.** VoIP Services Lines. 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 Cloud Services are used, or who use the Cloud Services, of the non-availability of 911 or other emergency dialling.

**7.6.** Security Features. If the Cloud Services will be used to transmit or process Personal Data, Customer will ensure that all Personal Data is captured and used solely via the use of security features made available by Genesys.

**7.7.** Recordings. Customer acknowledges that use of recordings is solely within Customer's 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: (a) 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; or (v) recordings are encrypted at all times. Customer shall not modify, disable, or circumvent the recording encryption feature within the Cloud Services.

**8. Industry-Specific Certifications**. Genesys security and operational controls are based on Industry Standard practices and are certified to meet the guidelines of PCI, SOC 2 Type 2, ISO 27001, and HIPAA. Nevertheless, Customer is solely responsible for achieving and maintaining any industry-specific certifications required for Customer's business.

**9. Audit**. Subject to Genesys' reasonable confidentiality and information security policies, Customer or a qualified third party chosen by Customer, shall have the right, not more than once a year and upon thirty (30) days' written notice, to perform a security assessment of Genesys' compliance with the terms of these Cloud Security Terms, provided that Customer has demonstrated that it has a reasonable belief that Genesys is not in compliance. During normal business hours, Customer or its authorized representatives may inspect Genesys policies and practices implemented to comply with these Cloud Security Terms, which may include a site visit and a review of reasonable supporting documentation, provided that Customer agrees that such right shall not include the right to on-site inspections or audits of any of Genesys' subcontractors, including Genesys' third-party hosting facilities and equipment. No such assessment shall violate Genesys' obligations of confidentiality to other customers or partners or reveal Genesys' intellectual property. Any assessment performed pursuant to this Section shall not interfere with the normal conduct of Genesys' business. Genesys shall cooperate with any reasonable requests made by Customer during the course of such assessments. Genesys reserves the right to charge Customer a reasonable fee for Genesys' costs incurred (including internal time spent) in connection with any Customer assessments, whether the assessment was performed remotely or on-site.

## PureConnect Cloud

This security policy describes the minimum requirements for information security and data protection provided by Genesys to Customer related to the provision of Genesys PureConnect Cloud Services under the Master Agreement. This security policy is applicable 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 Master Agreements.

**1.8 Vulnerability and Patch Management**. Genesys will maintain a vulnerability management program based on industry standard practices that routinely assesses 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 Master 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 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 regarding 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 36 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 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 Master 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 Master 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 Master Agreement will be conducted a maximum of one (1) time during any twelve (12) month period during which this Master 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 3.0 certification for a specific deployment model within the U.S. Data Centers located in Carmel, Indiana and Englewood, Colorado. PCI certification does not extend to any other Data Center.

## Premise Support Security

This security policy describes the minimum requirements for information security and data protection provided by Genesys to Customer related to the provision of support for Genesys premises-based services under the Master Agreement. This security policy is applicable to the extent that Genesys has access and control over Customer Data.

### 1. SECURITY PROGRAM

**1.1 Security controls**. 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 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 Anti-Virus and Anti-Malware Protection**. Genesys will utilize industry standard anti-virus and anti-malware protection solutions to ensure that all servers in Genesys' 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.

**1.6 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 Master 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. USER ACCESS CONTROL

**2.1 Access Control**. Genesys will implement appropriate access controls to ensure only authorized users have access to Customer Data within Genesys' environment.

**2.2 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. The following guidelines will be followed regarding 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.

### 3. BUSINESS CONTINUITY AND DISASTER RECOVERY

**3.1 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. SECURITY INCIDENT RESPONSE

**4.1 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.

**4.2 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 36 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.

**4.3 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.

**4.4 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.

## Genesys DX Security

1. **Products and Services**

This document covers the security and privacy controls for Genesys DX. These products are live chat, omni-channel and conversational ai engagement services that help customer service staff directly engage with and assist visitors to their organization's website. Key features include conversation bots, real-time visitor monitoring, co-browsing, detailed reporting on chat activity and its overall effectiveness, the ability to define rules that automatically trigger the initiation of a live chat or bot engagements, the ability to route and distribute chats to improve efficiency, and the ability to monitor and manage customer conversations on various social channels, email and via SMS messages, knowledge management, and intent insights. Genesys DX offer multiple service tiers based on the number of engagements, users and features desired. Further, Genesys DX provides valuable built-in integrations and open APIs to allow customers to streamline operations with all of their systems working together.

2. **Product Architecture**

Genesys DX is a SaaS-based application delivered via a chat client and internet-based application server that writes to a database. The chat client functions inside the visitor's browser making https calls and maintaining a web socket connection to the application server. Agents connect using a .NET or web client over authenticated https to the same servers. Genesys Customer Content (as the term is defined in the Terms of Service) is processed on database servers and stored in an encrypted form.

**2.1 Storage and Service**

End-user interfaces traffic (incl. live chat with an agent) is handled by co-located servers with Equinix as well as on Amazon Web Services. Customers can choose to store their service in Europe, USA or India. Access to infrastructure is limited to authorized individuals of the Development Operations team.

According to customers geo-location, the Genesys DX ai Chatbot data center is handled by co-located servers with Equinix as well as on Amazon EC2 cloud within Europe, USA or India, and accessed by the Network Operations Team for support purposes with no access to customer content.

All touch points and APIs are processed by our application servers, that mediate access to storage servers which can only be accessed from within our secured network.

Our back-office management interface, hosted on co-location facilities with Equinix and Switch, is a secured and encrypted web console (using TLS and SSL encryption). Credentials are encrypted and use a strict password complexity policy to ensure only your authorized personnel can access your knowledge.

3. **Genesys DX Technical Security Controls**

Genesys employs industry standard technical controls appropriate to the nature and scope of the Services designed to safeguard the Service infrastructure and data residing therein.

**3.1 Logical Access Control**

Logical access control procedures are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or "least privilege") access to specified Genesys systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

Administrative controls set or restrict agent/user access to certain actions, setup areas, departments and folders.

The Genesys operational system is only accessible with an authorized username (or email) and password combination. Usernames (and emails) must be unique throughout the entire Genesys system, and minimum password length and complexity requirements are enforced. Enhanced password controls, including initial login reset, rotation, aging, non-reuse and incorrect password lockout, are available to administrators in the user configuration settings. Single Sign On (SSO) integration is available to Enterprise subscribers using SAML 2.0-compliant user management systems.

User logins to Genesys are logged and reported within the application. Access to these reports can be restricted using permission settings.

**3.2 Perimeter Defense and Intrusion Detection**

The Genesys on-premises and Genesys components and services running on third-party cloud providers' network architecture is segmented into public, private, and Integrated Lights Out (iLO) management network zones. The public zone contains internet- facing servers. All traffic that enters this network must transit a firewall. Only required network traffic is allowed; all other network traffic is denied, and no network access is permitted from the public zone to either the private or iLO management network zones.

The private network zone hosts application level administrative and monitoring systems, and the iLO management network zone is for hardware and network administration and monitoring. Access to these networks is restricted to authorized employees via two-factor authentication.

Moreover, Genesys employs perimeter protection measures, including a third party, cloud-based distributed denial of service (DDoS) prevention service, designed to prevent unauthorized network traffic from entering our product infrastructure.

**3.3 Data Segregation**

Genesys leverages a multi-tenant architecture logically separated at the database level, based on a user's or organization's Genesys account. Only authenticated parties are granted access to relevant accounts.

New Genesys customers can use the Data Residency Option to choose whether their Content will be stored in Genesys' on-premises United States or European data centers and third-party cloud providers' United States, European and Indian regions hosted and replicated in separate regions to meet cross-border data privacy and residency requirements.

**3.4 Physical Security**

Data center Physical Security

Genesys contracts with Data centers and third-party cloud providers to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation, and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant Data center
- Scheduled maintenance and validation of all critical security and environmental controls

Genesys and third-party providers limit physical access to production data centers to authorized individuals only. Access to an on-premises server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by Technical Operations. Genesys management reviews physical access logs to on-premises data centers and server rooms on at least a quarterly basis. Additionally, physical access to data centers is removed upon termination of previously authorized personnel.

### 3.5 Data Backup, Disaster Recovery, Availability

Genesys has near instantaneous fail-over capabilities for most failure scenarios. The production Data centers utilize redundant high-speed network connections. There are pools of redundant servers across geographically distant data centers. Load balancers distribute network traffic among these servers and maintain the availability of these servers in the event of server or Data center failures.

The Genesys database is synchronized every five minutes to another data center. In addition, a differential back-up is completed nightly, and full backups are conducted every weekend. The backup database is stored with the same encryption as the original. Backups are retained on-premises for one week. In the event of a complete failure of the data center hosting the primary database, Genesys is designed to be restored within fifteen minutes.

### 3.6 Malware Protection

Malware protection software with audit logging is deployed on all Genesys servers. Alerts indicating potential malicious activity are sent to an appropriate response team.

### 3.7 Encryption

Genesys maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other relevant standards groups. This standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

**In-Transit Encryption**

All network traffic flowing in and out of Genesys data centers, including all Customer Content, is encrypted in transit with 256-bit AES encryption.

**At-Rest Encryption**

Genesys encrypts all Customer Content at rest with 256-bit AES encryption.

### 3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams, as well as management.

### 3.9 Logging and Alerting

Genesys collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

## 4. Organizational Controls

Genesys operates a comprehensive set of organizational and administrative controls to protect the security and privacy posture of Genesys.

### 4.1 Security Policies and Procedures

Genesys maintains and implements a comprehensive set of security policies and procedures aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

### 4.2 Standards Compliance

Genesys complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certifications and external audit reports:

- International Organization for Standardization – ISO/IEC 27001:2013 Information Security Management System (ISMS) Certification
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Sarbanes-Oxley Act (SOX)

- Payment Card Industry Data Security Standard (PCI DSS) Compliance for Genesys' eCommerce and Payment Environments

### 4.3 Security Operations and Incident Management

Genesys' Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with Genesys' critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services, including Genesys. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the Genesys intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

### 4.4 Application Security

Genesys' application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modelling, static code analysis, dynamic analysis, and system hardening.

### 4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

### 4.6 Security Awareness and Training Programs

New hires are informed of security policies and the Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

Genesys employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire on-boarding kits, and awareness campaigns for securing data, devices, and facilities.

## 5. Privacy Practices

Genesys takes the privacy expectations of its Customers and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

### 5.1 Data Protection and Privacy Policy

Genesys is pleased to offer a comprehensive, global Data Processing Addendum (DPA), available in English and German, to meet the requirements of the GDPR, CCPA, and beyond and which governs Genesys' processing of Personal Data as may be located within Customer Content.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including: (a) data processing details, sub-processor disclosures, etc. as required under Article 28; (b) EU Standard Contractual Clauses (also known as the EU Model Clauses); and (c) inclusion of Genesys' technical and organizational measures. Additionally, to account for CCPA coming into force, we have updated our global DPA to include: (a) revised definitions which are mapped to CCPA; (b) access and deletion rights; and (c) warranties that Genesys will not sell our users' 'personal information.'

For visitors to our webpages, Genesys discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on our public website. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

### 5.2 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. The Service is compliant with the applicable provisions of the GDPR.

### 5.3 CCPA

Genesys hereby represents and warrants that it will follow the California Consumer Privacy Act (CCPA) and will implement and maintain the necessary controls to adhere to the applicable provisions of CCPA.

### 5.4 Transfer Frameworks

Genesys is aware of the European Court of Justice's decision with respect to the EU-U.S. Privacy Shield Framework and is actively monitoring the situation.

Genesys' privacy program and contracts have been designed to account for shifts in the regulatory landscape to avoid impacts to our ability to provide our services to you. The EU-U.S. Privacy Shield Framework was just one (of several) mechanism that Genesys relied on to lawfully transfer personal data. Therefore, Genesys offer in the following Transfer Frameworks.

#### 5.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (or "SCCs") are standardized contractual terms, recognized and adopted by the European Commission, whose primary purpose are to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law. Genesys has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. Genesys offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope Genesys services as part of its global DPA. Execution of the SCCs helps ensure that Genesys customers can freely move data from the EEA to the rest of the world.

### 5.5 Return and Deletion of Customer Content

At any time, Customers may request the return or deletion of their Content through standardized interfaces. If these interfaces are not available or Genesys is otherwise unable to complete the request, Genesys will make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Customer Content will be deleted within thirty (30) days of Customer request. Customer's Genesys Content shall automatically be deleted within ninety (90) days after the expiration or termination of their final subscription term. Upon written request, Genesys will certify to such Content deletion.

### 5.6 Sensitive Data

While Genesys aims to protect all Customer Content, regulatory and contractual limitations require us to restrict the use of Genesys for certain kind of information. Unless Customer has written permission from Genesys, the following data must not be uploaded or generated to Genesys:

- Government issued identification numbers and image of identification documents.
- Information related to an individual's health, including, but not limited to, Personal Health Information (PHI) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations.
- Information related to financial accounts and payment instruments, including, but not limited to, credit card data. One exception extends to explicitly identified payment forms and pages that are used by Genesys to collect payment for Genesys. Another exception is that Genesys allows customers to maintain PCI-DSS compliance, while using Genesys to process payments, through a third-party gateway, contingent on Customer's appropriate configuration of their Genesys environment.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political believes, organizational memberships, etc.

### 5.7 Tracking and Analytics

Genesys is continuously improving its websites and products using various third-party web analytics tools, which help Genesys understand how visitors use its websites, desktop tools, and mobile applications, what they like and dislike, and where they may have problems. For further details please reference our Privacy Policy.

## 6. Third Parties

### 6.1 Use of Third Parties

As part of the internal assessment and processes related to vendors and third parties, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates vendors that provide information security-based services including the evaluation of third-party hosting facilities. Legal and Procurement may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes.

Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by Genesys are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

### 6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, Genesys reviews relevant third party's terms and conditions and either utilizes Genesys-approved procurement templates or negotiates such third-party terms, where deemed necessary.

## ANNEX IV

### List of sub-processors

**EXPLANATORY NOTE:**

**This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).**

**The controller has authorised the use of the following sub-processors:**

Genesys Cloud services are hosted by third party data center providers. Premise services operate on systems controlled and operated by the Customer. Genesys may share personal data with any affiliated Genesys entities under common control with Genesys for troubleshooting and support. Genesys may utilize subprocessors, depending on what services, features, and functionality the customer utilizes. Additional subprocessors may be selected by Customer in a customized environment, and if so such subprocessor will be listed in a Statement of Work or Order Form. Customer acknowledges that signature of such Statement of Work or Order form constitutes written consent for use of such subprocessor named therein. Note that third party integrations, such as AppFoundry, require a direct relationship between the third party and the customer.

The subprocessors listed at the following website (along with its subsidiary companies) may be utilized, depending on what services and functionality is selected by the Customer. Customer acknowledges that changes to this website shall constitute notice of changes to subprocessors.

https://help.mypurecloud.com/articles/genesys-subprocessors/