DATA PROCESSING ADDENDUM

This Data Processing Addendum**("Addendum")** forms part of the Terms and Conditions and Privacy Policy **("Agreement")** entered into by and between **Free Call, Inc.** having its place of business at Free Call, inc. 3041 Mission St # 2091 San Francisco CA 94110 United States of America **("Provider")**and _____ (required) having its place of business _____ (required)**("Client"**) pursuant to which Provider provides services **("Services")** to Client.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not defined herein shall have the meaning set forth in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

All terms introduced in the Addendum shall comply with regular meaning enshrined in **General Data Protection Regulation EU 2016/679.**

In the course of providing the Services to Client pursuant to the Agreement, Provider may Process Personal Data on behalf of Client and the parties agree to comply with the following provisions with respect to any Personal Data.

1. Effectiveness and Instructions

1.1 Legal Authority. Client signatory represents to Provider that he or she has the legal authority to bind Client and is lawfully able to enter into contracts.

1.2 Termination. This Addendum will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder or by the Provider's Terms and Conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this Addendum or (iii) as agreed by the parties in writing.

1.3. This Addendum will be effective only if it is executed and submitted to Provider in accordance with paragraph 1.4. below and this paragraph 1.3. This Addendum will be effective only if all items identified as "required" in the initial part of the Addendum and on page 8 of this Addendum are completed accurately and in full, and the Addendum is signed by an authorized representative of Client. If Client makes any deletions or other revisions to this Addendum, then this Addendum will be null and void.

1.4. Instructions. This Addendum has been pre-signed on behalf of Provider. To enter into this Addendum, Client must:

a. complete the initial part of the Agreement above and complete the information on page 8 of this Addendum by providing Client's full legal entity name, address and date of signing;

b. complete the Addendum by signing it on page 8 of the Addendum;

c. submit the completed and signed Addendum to Provider.

2. Definitions

"Client Personal Data" means any Personal Data Processed by Free Call, Inc. (or a Sub-processor) on behalf of
Client pursuant to or in connection with the Agreement;

“Data Protection Laws” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, and the GDPR, applicable to the Processing of Client Personal Data under the Agreement which are applicable to Client.
“GDPR” means the 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)
“Sub-processor” means any person (including any third party service provider, but excluding an employee of Provider or any of itssub-processors) appointed by or on behalf of Processor to Process Personal Data on behalf of Client under the Agreement.
The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing", “Processor”, and "Supervisory Authority" shall have the same meaning as in the GDPR and shall be construed accordingly.

3. Processing of Personal Data

3.1 Roles of the Parties. This Addendum applies when Client’s Personal Data is processed by Provider. In this context, Client may act as “controller” or “processor” and Provider may act as “processor” or “sub-processor” with respect to Personal Data. The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Data Controller, Provider is a Data Processor and that Provider will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.
3.2 Client Authority. Client represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instruction set forth in Section 3.4 below on behalf of itself and that it is and will at all relevant times remain duly and effectively authorized to process Personal Data covered by this Addendum.
3.3 Client’s Processing of Personal Data. Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. Client’s instructions for the Processing of Personal Data shall comply with Data Protection Laws. In addition, Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.
3.4 Provider’s Processing of Personal Data.
(a) Provider shall only Process Client Personal Data for the purpose of the provision of the Services under the Agreement and in accordance with Client’s documented instructions which are consistent with the terms of the Agreement, unless Processing is required by Data Protection Laws to which Provider (or the applicable sub-processor) is subject, in which case Provider shall to the extent permitted by the Data Protection Laws inform Client of that legal requirement before the relevant Processing of that Client Personal Data.
(b) This Addendum, the Agreement and any Order Forms thereunder, are Client’s complete and final instructions to Provider for the Processing of Client Personal Data. Any additional or alternate instructions must be agreed upon separately.
(c) The following are deemed instructions of the Client to Provider: The processing of Client Personal Data (i) in accordance with the Agreement, this Addendum and any Order Forms under the Agreement, including without limitation with the transfer of Client Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Agreement.
3.5 Details of the Processing. The subject-matter of Processing of Client Personal Data by Provider is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Client Personal Data and categories of Data Subjects Processed under this Addendum, as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws), are further specified in Exhibit A to this Addendum, as may be amended by the parties from time to time.
3.6. Client agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Client Personal Data and any processing instructions it issues to Provider; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Provider to process Client Personal Data and provide the Services pursuant to the Agreement and this Addendum.

3.7. Client agrees that except as provided by this Addendum, Client is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Client's Data when in confidential transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Client Data uploaded to the Services.

3.8. Obligations of the Client

The Client agrees and warrants:

(a) that the processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the applicable Data Protection Laws (and, where applicable, has been notified to the relevant authorities of the Member State where the Provider is established or has its representative) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the Personal Data processing Services will instruct the Provider to process the Personal Data transferred only on the Client's behalf and in accordance with the applicable Data Protection Law;

(c) that the Provider will provide sufficient guarantees in respect of the technical and organisational security measures specified in Exhibit B to this Addendum;

(d) that after assessment of the requirements of the applicable Data Protection Law, the security measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that the Client is solely responsible for the data entered into the system and shall be fully capable to determine correctness and legality of such data.

(f) that the Client is responsible for providing any special measures necessary in case of special categories of data as for example sensitive data.

(g) that it will ensure compliance with section 3.8 a to f of this Addendum.

3.9. Obligations of the Provider

The Provider agrees and warrants:

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

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

(c) that it has implemented the technical and organisational security measures specified in Exhibit B;

(d) that it will promptly notify Client about:

(i) any legally binding request for disclosure of Personal Data by a law enforcement authority unless otherwise prohibited;

(ii) any accidental or unauthorised access, and

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

(e) to deal promptly and properly with all inquiries from Client relating to its processing of Personal Data.

4. Provider Personnel

Throughout the term of this Addendum, Provider shall restrict its personnel from Processing Client Personal Data without authorization by Provider and shall limit the Processing to that which is needed for the specific individual's job duties in connection with Provider's provision of the Services under the Agreement. Provider will impose appropriate contractual obligations on its personnel, including relevant obligations regarding confidentiality, data protection and data security.

Furthermore, Provider declares that the personnel that is able to access personal data of the Client is aware of data protection procedures and trained to react in line with the Addendum.

5. Sub-processors (Third Party Service Providers)

5.1 Appointment of Sub-processors. For the purpose of the appointment of Sub-processors, Client acknowledges and agrees that Provider may engage third-party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Client Personal Data.

5.2 List of Current Sub-processors and Notification of New Sub-processors. When requested by the Client, the Provider shall make available to Client an up-to-date list of all Sub-processors used for the processing of Client Personal Data. The list of Sub-processors that are currently authorized by Provider to access Personal Data may be listed on a website maintained by Provider.

5.3. At least 10 days before Provider authorizes and permits any new Sub-processors to access Personal Data, Provider will update the applicable website. Customer may object in writing to Provider's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Client may suspend or terminate the Agreement (without prejudice to any fees incurred by Client prior to suspension or termination).

5.4 Sub-processing Agreement; Liability. Provider has or shall enter into a written agreement with each Sub-processor (the "Sub-processing Agreement") containing data protection obligations not less protective than those in the Agreement and/or this Addendum with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Provider shall be liable for the acts and omissions of its Sub-processors to the same extent Provider would be liable if performing the services of each Sub-processor directly under the terms of this Addendum.

5.5 Copies of Sub-Processor Agreements. Provider shall provide to Client for review copies of the Sub-processor agreements as Client may reasonably request from time to time. The parties agree that all commercial information may be removed by the Provider beforehand.

6. Security

6.1 Adequate Measures. Taking into account 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, Provider shall in relation to the Client Personal Data, implement and maintain throughout the term of this Addendum, the technical and organizational measures set forth in Exhibit B (the "Security Measures"). Client acknowledges and agrees that it has reviewed and assessed the Security Measures and deems the appropriate for the protection of Client Personal Data.

6.2 Personal Data Breach Risk. In assessing the appropriate level of security, Provider shall take account of the risks that are presented by Processing, in particular from a Client Personal Data Breach

7. Data Subject Rights

7.1 Correction, Blocking and Deletion. Provider shall comply with any commercially reasonable request by Client to correct, amend, block or delete Client Personal Data, as required by Data Protection Laws, to the extent Provider is legally permitted to do so and technically capable to do so.

7.2 Measures to assist with Data Subject Rights. Taking into account the nature of the Processing, Provider shall assist Client by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Client's obligations, as reasonably understood by Client, to respond to requests to exercise Data Subject rights under the Data Protection Laws. To the extent legally permitted, Client shall be responsible for any costs arising from Provider's provision of such assistance.
7.3 Response to Requests. Provider:
(a) shall promptly notify Client if it or any Sub-processor receives a request from a Data Subject under any Data Protection Laws & Regulation in respect of Client Personal Data; and
(b) shall not and shall ensure that no Sub-processor responds to that request except on the documented instructions of Client or as required by Data Protections Laws to which Provider or Sub-processor is subject, in which case Provider shall, to the extent permitted by such Data Protections Laws inform Client of that legal requirement before it or the applicable Sub-processor responds to the request.

8. Personal Data Breach
8.1 Notification of Data Breach. Provider shall, to the extent permitted by law, notify Client without undue delay upon Provider or any Sub-processor becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information, to allow Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
8.2 Assistance to Client. Provider shall cooperate with Client and take such reasonable commercial steps to assist in the investigation, mitigation and remediation of each such Personal Data Breach.
8.3. Internal registration. Provider shall register all Personal Data Breach examples to improve data protection internally if applicable. Such registration may take the form of status page update.

9. Data Protection Impact Assessment and Prior Consultation
Provider shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law & Regulation, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, Provider or the Sub-processors

10. Return or Destruction of Personal Data.
10.1 Return or Deletion. Subject to the provisions of Section 10.2 below, at Client's election, made by written request to Provider, Provider shall, and shall procure that all Sub-processors:
(a) return a complete copy of all Client Personal Data to Client in standard format accepted by Provider; and
(b) delete and procure the deletion of Client Personal Data Processed by Provider or any Sub-processor. Provider shall comply with any such written request within 30 days, unless it is unworkable due to the purposes of processing.
10.2 Retention of Copies. Provider and each Sub-processor may retain Client Personal Data to the extent required by applicable European Union law or the law of an EU Member State and only to the extent and for such period as required by such laws and always provided that Provider shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in such law requiring its storage and for no other purpose.
10.3. Client agrees that after the termination or expiration of the Agreement their data may be stored as a backup for the time needed to secure (establish, investigate or defend) Client's and Provider's claims that may arise due to the performance of the Services (for the time it takes for the claims to be barred) or due to other reason required by law.

11. Audit.

11.1 Report on Compliance. Subject to the provisions of Section 11.3 below, at Client's written request, Provider will provide Client all information necessary to demonstrate compliance with this Addendum. The information provided will constitute Provider Confidential Information under the confidentiality provisions of the Agreement or a non-disclosure agreement, as applicable.

11.2. Provider uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which Provider provides the Services. This audit: (a) will be performed at least annually; (b) will be performed by independent third party security professionals at Provider's selection and expense; and (c) will result in the generation of an audit report ("Report"), which will be Provider's Confidential Information. If Client's Agreement does not include a provision protecting Provider's Confidential Information, then Reports will be made available to Client subject to a mutually agreed upon non-disclosure agreement covering the Report (an "NDA").

11.3. At Client's written request, Provider will provide Client with a confidential Report so that Client can reasonably verify Provider's compliance with the security obligations under this Addendum. The Summary Report will constitute Provider's Confidential Information under the confidentiality provisions of the Agreement or the NDA, as applicable.

11.4 Audit. If the results of such review are not sufficient for Client and the Report does not cover issues requested by Client, Client may carry out its own audit. In such case Provider shall allow for audits, including inspections, by any Client or an auditor mandated by Client in relation to the Processing of the Client Personal Data by Provider or Sub-processors in accordance with Sections 11 to this Addendum.

11.5 Process. The parties agree that the audits shall be carried out in accordance with the following specifications:

(a) Client should contact Provider to request an audit of the procedures relevant to the protection of Personal Data. Before the commencement of any such audit Client should review the Reports.

(b) Client shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Provider or Sub-processor premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

(c) Before the commencement of any such audit, Client and Provider shall mutually agree upon the scope, timing, and duration of the audit.

(d) Provider or Sub-processor need not give access to its premises for the purposes of such an audit or inspection:

(i) to any individual unless he or she produces reasonable evidence of identity and authority;

(ii) outside normal business hours at those premises; or

(iii) for the purposes of more than one audit or inspection, in respect of Provider or each Sub-processor, except for any additional audits or inspections which: (A) Client reasonably considers necessary because of genuine concerns as to Provider's or applicable Sub-processor's compliance with this Addendum; or (B) Client is required or requested to carry out by Data Protection Law and Regulation, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory; where Client has identified its concerns or the relevant requirement or request in its notice to Provider.

11.6 Following the Audit:

(a) If Client chooses to conduct an independent audit rather than rely on a current available reports or current audits, if applicable and available, Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit.

(b) Client shall promptly notify Provider with the full results of an audit (including any non-compliance discovered during the course of an audit).

12. Transfer of Data. Privacy Shield

12.1. The parties agree that this Addendum, the Agreement and any Order Forms thereunder, are Client's complete and final instructions to Provider for the Processing of Client Personal Data. Any additional or alternate instructions must be agreed upon separately. Provider agrees and warrants to process the personal data only on behalf of the Client and in compliance with its instructions. If it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Client of its inability to comply, in which case the Client is entitled to suspend the transfer of data and/or terminate the contract.

12.2. Privacy Shield. To the extent that Provider processes any Client Personal Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Provider shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Client Personal Data by virtue of having self-certified its compliance with Privacy Shield. Provider agrees to protect such Personal Data in accordance with the requirements of the Privacy Shield Principles. If Provider is unable to comply with this requirement, Provider shall inform Client.

12.3. Provider may transfer and process Client Personal Data anywhere in the world where Provider, its affiliates or its Sub-processors maintain data processing operations. Provider shall at all times provide an adequate level of protection for the Client Personal Data processed, in accordance with the requirements of Data Protection Laws.

12.4. If Provider is not Privacy Shield certified with the U.S. Department of Commerce, Provider agrees to accept additional data privacy and security terms as instructed by Client from time to time as necessary to address applicable data protection, privacy or security laws regarding Personal Data, including but not limited to the European Commission Standard Contractual Clauses for Data Protection (2010/87/EU).

13. Indemnification; Liability

13.1 If one party is held liable for a violation of this Addendum committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred in accordance with the provisions of the Agreement.

13.2. In case of violation of the provisions of the Addendum or any other legal acts by Provider, as a result of which Client will be legally bound by a court judgment or administrative decision to pay damages, compensation or fine, Client reserves the right to claim damages against the Provider for this reason.

13.3. The Provider shall be liable for any damage caused to third parties due to the improper processing by the Provider of Personal Data entrusted to him by Client excluding the situation where the damage is the result of an action or omission for which Provider is not responsible.

13.4. Liability Cap. Provider's entire liability to Client arising out of or related to this Addendum shall not exceed the amount actually paid by Client to Provider during the prior twelve (12) months under the Agreement.

14. Profiling

14.1 Client gives its consent to the profiling of Personal Data that was given to Provider, for the purpose of proper maintenance and providing the Service to Client. Client agrees that the profiling of data shall serve, in particular, the purpose of providing Client with content that is accurate and consistent with the scope of the Service used by Client. Client acknowledges that it has the right not to be profiled. In such case the request can be made at any time at support@freecallinc.com. The Parties undertake reasonable steps and efforts to eliminate profiling however in case of withdrawing the consent, Client is aware and acknowledges that it is tantamount to the lack of possibility to provide the service. Withdrawing the consent is tantamount to the termination of the Agreement.

[Remainder of Page Intentionally Left Blank; Signature Pages to Follow]

EXECUTED by and on behalf of:
Provider
Free Call, Inc.
Name: Daniel Hristov
Role: Chief Operating Officer
Email: support@freecallinc.com

Date:

EXECUTED by and on behalf of
Client
.....
.....
Name: (required)
Role: (required)
Signature date: (required)
Email: (required)

EXHIBIT A TO DATA PROCESSING ADDENDUM: DETAILS OF PROCESSING

• Duration of the Processing:

The duration of data processing shall be for the term agreed between Client and Provider in the Agreement (or an applicable Order Form) which is the duration of the Agreement and after the termination or expiration of the Agreement for the time it takes for the claims to be barred. The objective of the data processing is performing Services and securing (establishing, investigating or defending) claims that may arise due to the performance of the Services.

• Nature and purpose of the Processing:

The scope and purpose of processing of the data subjects' personal data (specified in the Agreement) is:

- to provide, maintainand facilitatethe Provider's Services as well as to ensure safe and guaranteed Service performance, upgrade and improve the functionality of the Services;
- to provide Client with access to its Personal Data (including chat content) and maintain this access via standard API methods for the duration of paid usage of Services (active subscription) as well as after the subscription is expired (inactive subscription), until the Service is fully terminated by a written request (in accordance with the Agreement and this Addendum);
- tosecure (establish, investigate or defend) Client's as well as Provider's claims that may arise due to the Services.

• Categories of Data Subjects:

Data subjects include Client, Client's representatives and end-users including employees, contractors, collaborators, and Client's customers. Data subjects may also include individuals attempting to communicate or transfer personal information to users of Provider's Services. The data subjects exclusively determine the content of data submitted to Provider. Due to a full autonomy of data subjects regarding data entered to the system, Provider shall not be liable for the content entered to the system regardless if it constitutes personal data or not.

• Types of Client Personal Data:

The proceeded personal data includes email, first name and last name, address, title, contact details, username, chat history, financial information (credit card details, account details, payment information); employment details (employer, job title) and other data in an electronic form provided in the context of Provider's Services (specified in the Agreement).

EXHIBIT B TO DATA PROCESSING ADDENDUM: SECURITY MEASURES

1. Personnel. Provider's personnel (employees and contractors) will not process customer data without authorization. Personnel are obligated to maintain the confidentiality of any customer data and this obligation continues even after their engagement ends. Provider has limited the access of personnel to personal data to the minimum necessary to provide the service and performance maintenance.

2. Data Privacy Contact

Free Call, Inc.
3041 Mission St # 2091 San Francisco CA 94110
United States of America
Email: support@freecallinc.com

3. Technical and Organization Measures. Provider has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

3.1 Organization of Information Security.

Duty of Confidentiality. Provider's personnel with access to customer data are subject to confidentiality obligations.

3.2 Risk Management.

Provider conducts regular testing and monitoring of the effectiveness of its safeguards, controls, systems, including conducting penetration testing and risk assessment. Provider implements measures, as needed, to address vulnerabilities discovered in a timely manner.

3.3 Storage.

Provider's database servers are hosted in a data center operated by a third party vendor. Provider maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to customer data.

3.4 Asset Management.

(a) Asset Inventory. Provider maintains an inventory of all media on which customer data is stored. Access to the inventories of such media is restricted to authorized personnel.

(b) Asset Handling.

(i) Provider's employees are required to utilize encryption to store data in a secure manner and are required to use two-factor authentication to access Free Call, Inc. network.

3.5 Software Development and Acquisition: For the software developed by Provider, Provider follows secure coding standards and procedures set out in its standard operating procedures.

3.6 Change Management: Provider implements documented change management procedures that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for the Provider's software, information systems or network architecture. These change management procedures include appropriate segregation of duties.

3.7 Third Party Provider Management: In selecting third party providers who may gain access to, store, transmit or use customer data, Provider conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

3.8 Human Resources Security. Provider informs its personnel about relevant security procedures and their respective roles, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

3.9 Physical and Environmental Security.

(a) Physical Access to Facilities. Provider limits access to facilities where information systems that process customer data are located to identified authorized individuals who require such access for the performance of their job

function. Provider terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to customer data.

(b) Protection from Disruptions. Provider uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.

3.10 Communications and Operations Management.

(a) Security Documents. Provider maintains security documents describing its security measures and the relevant procedures.

(b) Data Recovery Procedures.

(i) On an ongoing basis, the Provider maintains multiple copies of customer data from which it can be recovered.

(ii) Provider stores copies of customer data and a data recovery procedures in a different place from where the primary computer equipment processing the customer data is located.

(iii) Provider has procedures in place governing access to copies of customer data.

(iv) Provider has anti-malware controls to help avoid malicious software gaining unauthorized access to customer data.

(c) Encryption; Mobile Media. Provider uses HTTPS encryption on all data connections. Provider restricts access to customer data in media leaving its facilities. Provider further has a destruction policy for hardware in the data center that stores customer data.

(d) Event Logging. Provider logs the use of data-processing systems. Logs are maintained for at least 10 days.

3.11 Access Control.

(a) Records of Access Rights. Provider maintains a record of security privileges of individuals having access to customer data.

(b) Access Authorization.

(i) Provider maintains and updates a record of personnel authorized to access systems that contain customer data.

(ii) Provider deactivates authentication credentials of employees or contract workers immediately upon the termination of their employment or services

(c) Least Privilege.

(i) Technical support personnel are only permitted to have access to customer data when needed for the performance of their job function.

(ii) Provider restricts access to customer data to only those individuals who require such access to perform their job function.

(d) Integrity and Confidentiality.

(i) Provider instructs its personnel to disable administrative sessions when leaving the Provider's premises or when computers are unattended.

(ii) Provider's stores passwords in a way that makes them unintelligible while they are in force.

(e) Authentication.

(i) Provider uses commercially reasonable practices to identify and authenticate users who attempt to access information systems.

(ii) Where authentication mechanisms are based on passwords, the Provider requires the password to be at least six characters long.

(iii) Provider allows using double authorization (2-factor authentication) of access to the systems.

(iv) Provider ensures that de-activated or expired identifiers are not granted to other individuals.

(v) Provider maintains commercially reasonable procedures to deactivate passwords that have been corrupted or inadvertently disclosed or pursuant to a number of failed login attempts.

(f) Network Design. Provider has controls to avoid individuals assuming access rights they have not been assigned to gain access to customer data they are not authorized to access.

3.12 Network Security.

(a) Network Security Controls. Provider's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.

(b) Antivirus. Provider's implements endpoint protection on its hosting environments, including antivirus; which are continuously updated with critical patches or security releases in accordance with Provider's server change control procedures.

3.13 Information Security Incident Management.

(a) Record of Breaches. Provider maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and the procedure for recovering data.

(b) Record of Disclosure. Provider tracks disclosures of customer data, including what data has been disclosed, to whom, and at what time, unless prohibited by law.