DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereafter the "**Agreement**") is made on … and entered into by and between:

Avanquest North America Inc., having its registered office at 23801 Calabasas Road, Suite 2005, Calabasas CA 91302-1547, United States of America, hereinafter called "**Avanquest**" or "**Controller**"

and

Ingram Micro Philippines BPO LLC, having its registered office at …, hereinafter called "**Ingram Micro**" or **"Processor".**

Hereinafter also referred to individually as a "**Party**" and collectively as the "**Parties**"

WHEREAS:

A. Controller and Ingram Micro Inc. have entered into a Master Services Agreement dated September 26, 2013, and/or any associated addendum(s), amendments, statements of work(s) etc. which are governed by the Service Agreement ("**Service Agreement**"), and by which Ingram Micro Inc. provided services to Controller;
B. Ingram Micro Inc. and Controller has agreed to transfer and assign all of Ingram Micro Inc.'s rights, title and interests in the Services Agreement to Ingram Micro Philippines BPO LLC which agreed to assume all such duties and obligations under Services Agreement in accordance with the Assignment and Assumption Agreement effective as of March 29, 2022.
C. Processor may need to Process Personal Data on behalf of Controller in the course of providing the Services to Controller pursuant to the Service Agreement;
D. Regarding the Processing of Personal Data the provisions of this Data Processing Agreement supersede all previous understandings and agreements between the Parties.
E. This Data Processing Agreement will apply only if and to the extent Ingram Micro is Processing Personal Data on behalf of Avanquest pursuant to the execution of the Services under the Service Agreement.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

"**Attachment**" means each annex, exhibit, schedule or other attachment to this Data Processing Agreement which forms part of the agreement

"**Data Subject**" means any identified or identifiable person or legal entity (if the case may be under the applicable legislation) to whom Personal Data relates; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural and/or social identity of that person.

"Data Controller" or "Controller" means the legal person which alone or in conjunction with others, determines the purposes and means of the Processing of Personal Data, and which hereunder is Avanquest;

"Data Processing Agreement "or "Agreement" means this agreement including its Attachments;

"**Data Protection Laws and Regulations**" means all applicable laws, directives, ordinances, rules, regulations etc. including but to the extent applicable European or local country privacy laws and regulations, such as the GDPR, privacy laws and regulation of the United States of America and, the data protection or privacy laws of any country applicable to the Processing of Personal Data under this Agreement and the Service Agreement;

"Data Security Breach" means any incident involving the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of or access to Personal Data, under this Agreement.

"Data Transfer" or **"Transfer"** means any cross-border communication of Personal Data regardless of the format, any storage of Personal Data on data-bases hosted in different countries, any access to Personal Data hosted in a different country or the use of Personal Data by Third Parties;

"**GDPR**" or **"General Data Protection Regulation"** means the EU General Data Protection Regulation 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;

"**EEA**" means the European Economic Area which consists of all countries of the European Union, Liechtenstein, Norway and Iceland;

"**Service Agreement**" means the main agreement for the provision of Services between Controller and Processor as provided under section Whereas;

"**Personal Data**" means any information relating to an identified or identifiable natural person, household, or legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), received and processed by Processor on behalf of and for Controller under this Agreement and in course of providing the Services;

"**Processing" "Process" or "Data Processing"** means any operation or any set of operations concerning Personal Data, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, dissemination, disclosure by means of transmission, distribution or otherwise making available in any other form, merging, linking, as well as restriction, erasure or destruction of data;

"**Data Processor**" or "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, and which under this Agreement is Ingram Micro;

"**Services**" means all services Processor provides as agreed to in the Service Agreement;

"Standard Contractual Clauses" means the contractual clauses pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

"Sub-processor" means any data processor authorized under the Agreement and engaged by Processor in the course of providing the Services as a subcontractor to the Processor.

"Supervisory Authority" means an independent public authority established in a particular country responsible for monitoring the compliance with the Data Protection Laws and Regulations within such country, in order to protect the fundamental rights and freedoms of natural persons in relation to processing.

"Third Party" means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor, Processor's affiliates or authorized Sub-processors;

2. GENERAL

The Parties shall at all times comply with the applicable data protection legislation and privacy laws, including where applicable the GDPR. The Parties acknowledge and agree that with regard to the Processing of Personal Data hereunder, Avanquest is the Data Controller and Ingram Micro is the Data Processor.

The subject-matter of Processing of Personal Data by the Processor is the performance of the Services pursuant to the Service Agreement.

3. PROCESSING OF PERSONAL DATA AND CROSS-BORDER DATA TRANSFER

3.1 Attachment 1 contains an overview of categories of Data Subjects, categories of Personal Data and the purposes of Processing Personal Data, under this Data Processing Agreement.

3.2 Processor shall Process and use the Personal Data for the purposes defined by the Controller as set out in Attachment 1 and in particular as necessary to (i) provide the Services, and (ii) exercise its rights or comply with its obligations under this Agreement, the Service Agreement or the applicable laws**.** The Parties agree that reasonable amendments to Attachment 1 might take place upon mutual written agreement by the Parties from time to time as necessary to meet legal and data protection requirements.

3.3 Processor will Process Personal Data on behalf of Controller i) in accordance with Controller's documented instructions in relation to the Processing of Personal Data as part of providing the Services under the Service Agreement, ii) in accordance with this Data Processing Agreement and the applicable Data Protection Laws and Regulations as it relates to the Processing hereunder and/or (iii) as necessary to comply with legal obligations to which Processor or its affiliated companies are subject. Parties agree that this Agreement and the Service Agreement constitute Controller's documented instructions regarding Processor's Processing on behalf of Avanquest. Additional instructions outside the scope of the documented instructions herein may be provided separately in writing by an authorized representative of the Avanquest but such change will be subject to Processor's prior written agreement before entering into force. For the avoidance of doubt, Controller will ensure that its instructions for the Processing of Personal Data shall comply with the applicable laws. If, however, at any time during the execution of this Agreement and the Service Agreement, Processor establishes that Controller's instructions appear in any way to be unlawful or non-compliant with the applicable laws, Processor shall without undue delay notify this to Controller and wait for further instructions. In such event, if necessary, Processor reserves the right to suspend the Processing until Controller issues further lawful instructions.

3.4 In the event a legal requirement prevents Processor from complying with Controller's instructions or requires Processor to Process the Personal data for a particular purpose or to disclose the Personal Data to a Third Party, Processor shall, to the extent allowed to do so by the applicable laws, inform Controller in writing of the relevant legal requirement before carrying out the relevant Processing activities and reasonably co-operate with Controller regarding the manner of such disclosure.

3.5 Controller acknowledges and agrees that Processor may need to transfer, disclose or otherwise permit access to the Personal Data to its affiliates or sub-contractors located in different countries for the purposes described under Agreement. Upon signing this Data Processing Agreement, Controller grants Processor a general authorization to Process in, Transfer, disclose or to otherwise permit access to the Personal Data including to its Sub-processors, from different countries including outside the EEA, Switzerland and the United Kingdom ("**UK**") for the purposes hereunder or under the Service Agreement. Notwithstanding the above, Processor will provide Controller with an overview of the countries in which the Personal Data is Processed or Transferred to. Upon signing this Agreement Controller agrees to the Transfer locations listed under Attachment 1 of this Agreement.

Notwithstanding the above Processor reserves the right to amend the Transfer locations and/or Sub-processors used with a thirty (30) days' advance written notice to Controller, which notice may be provided by e-mail or upon receipt by certified courier to the Controller address in the introduction of this Agreement. Avanquest has the right to object. It is expressly agreed by the Parties, that if Controller does not raise any objections to such changes or does not provide any answer until the expiration of the 30 days' time frame from the date of the written notice from Processor, such changes shall be deemed accepted by Controller. Controller agrees not to unreasonably and unjustifiably object to Processor's request. If Controller objects to a particular Transfer, Controller shall cooperate with Processor in good faith in remedying the situation in order to ensure the continuity of the Services. In the event, Parties cannot find a solution, they will have the right to terminate the Service Agreement for convenience in accordance with each Party's respective rights and obligations for termination for convenience under section 7 of the Service Agreement. In addition, all amounts due to Ingram Micro under this Agreement or the Service Agreement up until the effective date of such termination shall become immediately due and payable.

For the avoidance of doubt, in such event Processor will not be held liable and considered in breach of its

obligations under the Service Agreement or this Agreement due to any delays or non-performance of the Services resulting from the objection of Controller to any Transfer of Personal Data.

3.6 For Personal Data originating from the European Union and subject to the GDPR, if applicable, Parties agree and certify that any disclosure, access or Data Transfer outside the EEA of such Personal Data under this Agreement including to the Processor will be performed in compliance with the applicable Data Protection Laws and Regulations, the provisions set forth in this Data Processing Agreement and only upon implementing an adequate and legally valid data transfer safeguard mechanism as provided by the GDPR, such as by entering into the appropriate module of the Standard Contractual Clauses.

3.7 Controller warrants and represents that it will not unlawfully provide or transfer any Personal Data for Processing by Processor and that any Personal Data provided to Processor for Processing has been collected and obtained lawfully, using valid legal grounds and in compliance with the principles related to the processing of Personal Data as provided under the Data Protection Laws and Regulations, such as where needed, the Data Subject has given its consent to the Processing of its Personal Data by Processor. Controller also acknowledges and agrees that it has the sole responsibility of obtaining all necessary consents for the Processing of Personal Data under this Data Processing Agreement and thereby warrants and represents that where such consent is needed, Controller has obtained Data Subject's consent and upon written request by the Processor, copies of such consents will be provided to Processor.

3.8 Processor: (i) represents and warrants that where the California Privacy Rights Act ("CPRA") applies to the Processing, it understands the restrictions and prohibitions of the CPRA on selling Personal Data and on collecting, retaining, using, or disclosing Personal Data outside of a direct business relationship, and that Processor will comply therewith.

3.9 Processor: (i) represents and warrants that it has no reason to believe any of the Data Protection Laws and Regulations prevent it from performing the Services under the Service Agreement.

3.10 Where required under the applicable Data Protection Laws and Regulations and taking into account the nature of the Processing and the information available to the Processor, upon Controller's request, Processor shall provide Controller with reasonable cooperation and assistance needed to fulfill Controller's obligations under the Data Protection Laws and Regulations, such as to carry out data protection impact assessments or prior consultation with the Supervisory Authority, but only if and to the extent the Controller does not otherwise have access to the relevant information and to the extent such information is available to Processor. Controller shall reimburse Processor the reasonable costs of that cooperation and assistance.

4. RELIABILITY OF STAFF

Processor shall ensure that its personnel engaged in the Processing of Personal Data under this Data Processing Agreement, have received appropriate training on their responsibilities, necessary to comply with the Data Protection Laws and Regulations. Processor shall ensure that the access to Personal Data is limited to those personnel who requires such access to perform the Services under this Data Processing Agreement and the Service Agreement.

5. SECURITY OF PERSONAL DATA

5.1 Processor shall maintain commercially reasonable and appropriate technical and organizational security measures to ensure the security, availability, confidentiality and integrity of its computers, other information systems and services, and to protect Personal Data under this Agreement, against accidental, unauthorized or unlawful destruction, disclosure, coping, use, loss, alteration, or access or any other form of unlawful or unauthorized Processing in accordance with the applicable Data Protection Laws and Regulations.

5.2 Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the nature of Personal Data as well as the risk and severity for the rights and freedoms of natural persons, Processor will ensure that its security measures ensure a level of security appropriate to the risks presented by the Processing of Personal Data. Processor shall maintain such security measures and comply with the Data Protection Laws and Regulations for as long as it is Processing the

Personal Data, and this Agreement and the Service Agreement are not expired or terminated.

5.3 The technical and organizational security measures Processor has implemented are specified in Attachment 2 to this Data Processing Agreement. Controller agrees that the measures included in Attachment 2 are sufficient to ensure an appropriate level of security of the Personal Data.

6. AUDITS

6.1 Controller has the right, at its own costs, to audit or have an independent third-party auditor, as Controller may from time to time designate in writing, to perform an audit on its behalf in order to audit Processors' compliance with its obligations under the Data Processing Agreement and the applicable Data Protection Laws and Regulations. Any agreed upon third-party auditor will be subject to a non-disclosure agreement with Processor prior to any audit. Parties will agree on the scope, duration and time of the audit reasonably in advance. Processor shall provide Controller, for the purpose of the audit and upon written request, with all information necessary to demonstrate compliance with Processor's obligations under this Data Processing Agreement, excluding any confidential information, business sensitive information, trade or business secrets, third-party confidential information, information, documents or records relating to the business relations of Processor with any third party or the documents or records already audited by the Controller during the previous twelve (12) months. Processor shall ensure reasonable cooperation in the performance of the audit.

6.2 Controller may perform such audits no more than once every calendar year and upon providing to Processor a prior written notice of at least 30 business days. Controller shall carry out any inspection at mutually agreeable date, during normal working hours and without interfering with the course of Processor's business.

6.3 Recommendations and/or required alterations following from the audits will be assessed and applied by Processor after having consulted Controller.

7. SECURITY BREACHES AND NOTIFICATION

7.1 If the Processor becomes aware of any incident involving the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of or access to Controller's Personal Data, the Processor shall notify the Controller by email to legal@planetart.com without undue delay and as soon as reasonably possible about the Data Security Breach related to the Processing of Personal Data under this Agreement. Processor shall investigate and provide the Controller with sufficient information related to the Data Security Breach to the extent such information is already available to it, in order to allow Controller to meet any legal obligation if applicable to inform Data Subjects or the Supervisory Authority of the Data Security Breach under the applicable Data Protection Laws and Regulations.

7.2 To the extent such information is available to the Processor, it will provide Controller : (i) the categories of Data Subject whose data was accessed, compromised, or exfiltrated in the Data Security Breach; (ii) a brief description of what happened, including, without limitation where possible, the date of the Data Security Breach and the date of its discovery; (iii) a description of the categories of Personal Data that were involved in the Data security Breach; (iv) a description of the likely consequences of the Data Security Breach (v) a brief description of what Processor is doing or plans to do to investigate the Data Security Breach, mitigate any consequences of the breach and to prevent future Data Security Breaches; (vi) contact information for a designated person at Processor for further communications with Avanquest regarding the incident.

7.3 In case of a security incident Processor will promptly take adequate measures to mitigate the consequences of the incident and to prevent future incidents and will ensure reasonable cooperation to Controller

7.4 Processor will neither make any public statements nor notify any Data Subject or government authorities with respect to such Data Security Breach, except those that have been expressly and

unambiguously agreed to by Avanquest, unless required otherwise by the Data Protection Laws and Regulations or other applicable laws, and then only to the extent so required.

8. DATA SUBJECTS REQUESTS

Processor shall promptly notify Controller if it receives a request from a Data Subject to exercise its rights or any other Data Subject request, under the applicable Data Protection Laws and Regulations. Processor will not respond to any such Data Subject request without Controller's prior written consent and will only do so in accordance with Controller's instructions, except as necessary to confirm that the request relates to Controller. Processor shall provide Controller with all reasonable cooperation and assistance in order to enable Controller to comply with its legal obligations in relation to the handling of Data Subject requests within the statutory time limits, to the extent that the Processor is legally permitted to do so and provided that such Data Subject Requests are exercised in accordance with the applicable Data Protection Laws.

9. SUB-PROCESSOR

9.1 Processor shall not subcontract any of its Processing operations regarding Controller's Personal Data without the prior written consent of Controller which consent shall not be withheld in case of a reasonable request. Parties will include the relevant data of any Sub-processors in Attachment 1. Upon signing this Data Processing Agreement, Controller grants Processor a general authorization to sub-contract the Processing of Personal Data to Sub-processors located in different countries for the purposes agreed under this Agreement. A list of the Sub-processors used is available under Attachment 1. Upon signing this Agreement Controller agrees to the Sub-processors listed under Attachment 1 of this Agreement. Processor reserves the right to add, remove, or change the Sub-processors used with a thirty (30) day advance written notice to Controller, which notice may be provided by e-mail or upon receipt by certified courier to the Controller address in the introduction of this Agreement. It is expressly agreed by the Parties, that if Controller does not raise any objection to such changes or does not provide any answer to the request until the expiration of the 30 days' time frame from the date of the written notice from Processor, such changes shall be deemed accepted by Controller. Controller agrees not to unreasonably and unjustifiably object to Processor's request. If Controller objects to the appointment or replacement of a Sub-processor Controller shall cooperate with Processor in good faith in remedying the situation in order to ensure the continuity of the Services. In the event, Parties cannot find a solution, they will have the right to terminate the Service Agreement for convenience in accordance with each Party's respective rights and obligations for termination for convenience under section 7 of the Service Agreement. In addition, all amounts due to Ingram Micro under this Agreement or the Service Agreement up until the effective date of such termination shall become immediately due and payable. For the avoidance of doubt, in such event Processor will not be held liable and considered in breach of its obligations under the Service Agreement or this Agreement due to any delays or non-performance of the Services resulting from the objection of Controller to the use of the relevant Sub-processors.

9.2 Processor will carry out adequate due diligence on each Sub-processor to ensure that such Sub-processor is capable of providing at least the level of protection for Personal Data as is required by this Agreement. Processor shall only subcontract its Processing operations regarding the Personal Data by way of a written agreement signed between the Processor and the Sub-processor which is in accordance with the obligations and restrictions imposed on the Processor by the applicable Data Protection Laws and Regulations and the principles set forth in this Data Processing Agreement.

10. RETURN AND DELETION OF CONTROLLER'S DATA

10.1 Processor will retain the Personal Data for a duration as instructed by the Controller, and consistent with the retention periods in Attachment 1. Processor shall promptly and in any event within ninety (90) days of the date of cessation of any Services and the termination or expiration of the Service Agreement, return to Controller or, to the extent allowed by the applicable laws, delete all copies of Controller's Personal Data Processed on its behalf that might be in Processor's possession. Subject to the above, the return of Controller's Personal data and all its copies in Processor's possession shall be completed by secure file transfer in such format as is reasonably requested by Controller to Processor. The Parties agree that the Controller will bear all reasonable costs of Processor related to the return or the deletion of the Personal Data.

10.2 The Processor may retain Controller's Personal Data to the extent required by the applicable laws

and for such period as required by the applicable laws. Notwithstanding the above, when retaining Controller's Personal Data Processor shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is Processed only as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

11. INDEMNIFICATION

11.1 Controller shall indemnify and hold Processor harmless from any liability, losses, claims, penalties, damages, costs and expenses of whatever nature, including administrative fines imposed by the Supervisory Authority on Processor and arising out of any claims, actions, proceedings or settlements, resulting from the breach or non-compliance of Controller with the terms and conditions of this Data Processing Agreement and/or with the applicable Data Protection Laws and Regulations.

11.2 Processor shall:

(i) promptly notify Controller of any claim, investigation or other circumstances that come to its attention and that may lead to such liability, losses, claims, penalties, damages, costs and expenses to be imposed by the authorities;

(ii) act and communicate with the authority and cooperate as may be reasonably required by the Controller at Controller's cost in settling the claim;

12. LIMITATION OF LIABILITY

12.1 In no event will either Party be liable for consequential, exemplary, indirect, special, punitive or incidental damages arising out of or relating to this Agreement (including liability under any warranty or remedy in this Agreement).

12.2 Except for the indemnity obligations under section 11 here above, in no event will either Party's liability arising out of or relating to this Agreement, regardless of form of action, whether in contract, tort, negligence or otherwise, exceed the amounts paid (or in the case of Avanquest, payable) by Avanquest to Ingram Micro during the twelve (12) month period prior to the date on which the claim arises.

13. TERMINATION

The Data Processing Agreement will be effective as of the date of the last signature (the "Effective Date") and shall remain in force during the term of the Service Agreement. This Data Processing Agreement will terminate automatically with the termination or expiry of the Service Agreement.

14. MISCELLANEOUS

14.1 Except as expressly stated otherwise herein, in the event of changes in the Services or applicable Data Protection Laws and Regulations which will affect the Processing of the Personal Data and requires the amendment of the Data Processing Agreement in order for the Parties to be able to address the requirements and comply with the applicable laws, the Parties will consult with each other in good faith in order to amend the Data Processing Agreement. Any amendments to this Data Processing Agreement can solely be made in writing by duly authorized representatives of the Parties.

14.2 The Parties can at any time agree on amendments to the Attachments in writing and by adding a new version number to the Attachment.

14.3 If any provision of this Data Processing Agreement is found by any court or administrative body of competent jurisdiction to be void, invalid, illegal or otherwise unenforceable, all other terms and provisions of this Data Processing Agreement shall nevertheless remain in full force and effect, and the invalidity or unenforceability of such provision will not adversely affect the enforceability of any other provision of this Data Processing Agreement.

14.4 Except as expressly stated otherwise herein, in the event of a conflict between any of the terms of this Data Processing Agreement and its Attachments, the terms of this Data Processing Agreement shall

prevail. In case of any contradiction and inconsistency between the provisions of this Data Processing Agreement and the provisions set forth in the Service Agreement, the provisions of this Data Processing Agreement shall prevail.

14.5 The titles in this Agreement and the Attachments are for reference purposes only and shall not affect in any way whatsoever the meaning or interpretation of this Data Processing Agreement.

15. APPLICABLE LAW AND JURISDICTION

15.1 This Data Processing Agreement shall exclusively be governed by and construed in accordance with the laws governing the Service Agreement.

15.2 Any dispute, controversy or claim arising out of or in connection with this Data Processing Agreement or the breach, termination or invalidity thereof shall be settled and submitted to the competent courts having jurisdiction over the Service Agreement.

AGREED by parties to this Data Processing Agreement through their authorized signatories on the signing pages. This Data Processing Agreement may be signed in one or more counterparts and will form one Data Processing Agreement.

FOR CONTROLLER	**FOR PROCESSOR**
Name:	Name:
Title:	Title:
Date:	Date:
Signature……	Signature……

ATTACHMENT 1

A. Categories of Data Subjects

Processor will process Personal Data regarding the following categories of Data Subjects:
Customers of Avanquest

B. Categories of Personal Data

Personal Data processed by Processor will include:
Names, e-mail address, phone numbers, addresses, credit card info, billing address, delivery address, program data

C. Purposes of Processing Personal Data

The Personal Data will in any event be processed for the following purposes:
As necessary for the provision of the Services, such as for documentation & identification, callback, sending instructions via email or details regarding an order, processing orders for support code, checking order status of physical item, troubleshooting and issues replication etc.

D. Cross-Border Data Transfer and Data Processing locations

The Personal Data will be processed and transferred to the following countries outside the EEA:
Ingram Micro BPO Philippines LLC: the Philippines

E. Sub-processors

Processor has contracted the following Sub-processors: None

F. Retention Period

During the term of the Service Agreement and as necessary or required to comply with the applicable laws.

G. Contact details

The contact person regarding this Data Processing Agreement is:

Processor:
Name: Ingram Micro Data Protection team
E-mail address: privacy@ingrammicro.com

Controller:
Name:
E-mail address:

ATTACHMENT 2

Description of the organizational and technical security measures of the Processor in order to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and all other forms of unlawful Processing in accordance with applicable Data Protection Laws and Regulations

I. Organization of Information Security.

1) Security Ownership.

Data Processor has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

2) Security Roles and Responsibilities.

Data Processor personnel with access to Personal Data are subject to confidentiality obligations.

3) Risk Management Program.

Data Processor performed a risk assessment before processing the Personal Data.

4) Data Processor retains its security documents pursuant to its retention requirements after they are no longer in effect.

II. Asset Management.

1) Asset Inventory.

Data Processor maintains an inventory of all media on which Personal Data is stored. Access to the inventories of such media is restricted to Data Processor personnel authorized in writing to have such access.

2) Asset Handling.

A. Data Processor classifies Personal Data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption).

B. Data Processor imposes restrictions on printing Personal Data and has procedures for disposing of printed materials that contain Personal Data.

C. Data Processor personnel must obtain Data Processor authorization prior to storing Personal Data on portable devices, remotely accessing Personal Data, or processing Personal Data outside Data Processor facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing Personal Data from Data Processor's facilities.

III. Human Resources Security.

1) Security Training.

A. Data Processor informs its personnel about relevant security procedures and their respective roles. Data Processor also informs its personnel of possible consequences of breaching the security rules and procedures.

B. Data Processor will only use anonymous data in training.

IV. Physical and Environmental Security.

1) Physical Access to Facilities.

Data Processor limits access to facilities where information systems that process Personal Data are located to identified authorized individuals.

2) Physical Access to Components.

Data Processor maintains records of the incoming and outgoing media containing Personal Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Personal Data they contain.

3) Protection from Disruptions.

Data Processor uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

4) Component Disposal.

Data Processor uses industry standard processes to delete Personal Data when it is no longer needed.

V. Communications and Operations Management.

1) Operational Policy.

Data Processor maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data.

2) Data Recovery Procedures.

A. On an ongoing basis, Data Processor maintains multiple copies of Personal Data from which Personal Data can be recovered.

B. Data Processor stores copies of Personal Data and data recovery procedures in a different place from where the primary computer equipment processing the Personal Data is located.

C. Data Processor has specific procedures in place governing access to copies of Personal Data.

D. Data Processor reviews data recovery procedures at least every six months.

E. Data Processor logs data restoration efforts, including the person responsible, the description of the restored data and which data (if any) had to be input manually in the data recovery process.

3) Malicious Software.

Data Processor has anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks.

4) Data Beyond Boundaries.

A. Data Processor encrypts Personal Data that is transmitted over public networks.

B. Data Processor restricts access to Personal Data in media leaving its facilities (e.g., through encryption).

5) Event Logging

A. Data Processor logs the use of data-processing systems.

B. Data Processor logs access and use of information systems containing Personal Data, registering the access ID, time, authorization granted or denied, and relevant activity.

VI. Access Control.

1) Access Policy.

Data Processor maintains a record of security privileges of individuals having access to Personal Data.

2) Access Authorization.

A. Data Processor maintains and updates a record of personnel authorized to access Data Processor systems that contain Personal Data.

B. Data Processor deactivates authentication credentials that have not been used for a period of time not to exceed six months.

C. Data Processor identifies those personnel who may grant, alter or cancel authorized access to data and resources.

D. Data Processor ensures that where more than one individual has access to systems containing Personal Data, the individuals have separate identifiers/log-ins.

3) Least Privilege.

A. Technical support personnel are only permitted to have access to Personal Data when needed.

B. Data Processor restricts access to Personal Data to only those individuals who require such access to perform their job function.

4) Integrity and Confidentiality.

A. Data Processor instructs Data Processor personnel to disable administrative sessions when leaving premises Data Processor controls or when computers are otherwise left unattended.

B. Data Processor stores passwords in a way that makes them unintelligible while they are in force.

5) Authentication.

A. Data Processor uses industry standard practices to identify and authenticate users who attempt to access information systems.

B. Where authentication mechanisms are based on passwords, Data Processor requires that the passwords are renewed regularly.

C. Where authentication mechanisms are based on passwords, Data Processor requires the password to be at least eight characters long.

D. Data Processor ensures that de-activated or expired identifiers are not granted to other individuals.

E. Data Processor monitors repeated attempts to gain access to the information system using an invalid password.

F. Data Processor maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

G. Data Processor uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

6) Network Design.

A. Data Processor has controls to avoid individuals assuming access rights they have not been assigned to gain access to Personal Data they are not authorized to access.

VII. Information Security Incident Management.

1) Incident Response Process.

A. Data Processor 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 to whom the breach was reported, and the procedure for recovering data.

B. Data Processor tracks disclosures of Personal Data, including what data has been disclosed, to whom, and at what time.

2) Service Monitoring.

Data Processor security personnel verify logs at least every six months to propose remediation efforts if necessary.

VIII. Business Continuity Management.

1) Data Processor maintains emergency and contingency plans for the facilities in which Data Processor information systems that process Personal Data are located.

2) Data Processor's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its original state from before the time it was lost or destroyed.