DATA PROCESSING ADDENDUM

This Data Processing Addendum and its Addendums ("DPA") is supplemental to, and an integral part of, all contractual agreements, including the Master Agreement and Addendums available at www.connectwise.com/legal, as updated from time to time, by and between you and the entity and its Affiliates that you represent (hereinafter "you", "your", "Client", "Customer" or "MSP") and ConnectWise, LLC and its Affiliates ("ConnectWise") governing the data protection obligations ("Obligations") of ConnectWise and Client (collectively the "Parties") associated with the Offerings when EU GDPR or UK GDPR applies to Client's processing of Client Data.

I. RECITALS:

a) ConnectWise and Client have entered into a contractual agreement together with one or more accompanying statement(s) of work, schedule(s), purchase orders or order forms, or schedules, contracts or agreements, and/or schedules (collectively the " Agreement").

b) Pursuant to the Agreement, ConnectWise has agreed to provide to Client certain SaaS based managed offerings as described within the Agreement (the "Services" or "Offerings").

c) The Parties wish to enter into this DPA to define their respective Obligations associated with ConnectWise's provision of Offerings to Client.

d) In the case of any conflict or inconsistency with the terms of the Agreement and this DPA, this DPA will take precedence over the Agreement to the extent of such conflict or inconsistency.

II. IN CONSIDERATION OF THE MUTUAL PROMISES BELOW AND OTHER GOOD AND VALUABLE CONSIDERATION THE SUFFICIENCY OF WHICH ARE HEREBY ACKNOWLEDGED, IT IS AGREED:

1.0 Definitions

1.1 The terms of this DPA will follow the terms of the Agreement. Terms not otherwise defined in this DPA will have the same meaning as set forth in the Agreement.

a) **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

b) **"Applicable Data Protection Laws and Regulations"** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time, including, where applicable, EU/ UK Data Protection Law.

c) **"Authorized Affiliate"** means any of Client's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Client and ConnectWise, but has not signed its own Order Form with ConnectWise and is not a "Client" as defined under this DPA.

d) **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations. "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

e) **"Client"** means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates).

f) **"Client Data"** means what is defined in the Agreement as "Client Data" or "Your Data", provided that such data is electronic data and information submitted by, or for, Client in accordance with the Services. This DPA does not apply to Non-ConnectWise Applications as defined in the Agreement.

g) **"ConnectWise Group"** means ConnectWise, and its Affiliates engaged in the Processing of Personal Data.

h) **"Data Subject(s)"** means the identified or identifiable person to whom Personal Data relates.

i) **"EU/UK Data Protection Laws"** means (i) 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) (the "EU GDPR");(ii) the EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

j) **"Personal Data"** means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under Applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Client Data.

k) **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

l) **"Processor-to-Processor Clauses"** means Module Three of the Standard Contractual Clauses between processor to processor.

m) **"Processor"** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

n) **"Restricted Transfer"** means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

o) **"Standard Contractual Clauses"** means (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission Implementing Decision 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 ("EU SCCs"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("UK Addendum").

p) **"Sub-Processor"** means any Processor engaged by ConnectWise or a member of the ConnectWise Group.

q) **"Supervisory Authority"** means an independent public authority which is established by an EU Member State pursuant to the EU GDPR or, for the UK GDPR, the Information Commissioner's Office ("ICO") in the United Kingdom.

2.0 Processing of Personal Data

2.1 Roles of the Parties. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Controller (or, where Client is instructing ConnectWise on behalf of a third-party controller, a processor on behalf of that Controller), ConnectWise is the Processor and that ConnectWise or members of the ConnectWise Group will engage Sub-Processors pursuant to the requirements set forth below in Section 5, Sub-Processors of this DPA.

2.2 Client's Processing of Personal Data. In its use of the Service, Client shall Process Personal Data in accordance with the requirements of Applicable Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of ConnectWise as Processor. For the avoidance of doubt, Client's instructions (such instructions, where Client is a Processor, shall reflect the instructions of its Controller) for the Processing of Personal Data shall comply with Applicable Data Protection Laws and Regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired such Personal Data. Client specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data to the extent applicable under the CCPA.

2.3 ConnectWise's Processing of Personal Data. ConnectWise shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of, and only in accordance with, Client's documented instructions (such instructions, where Client is a processor, shall reflect the instructions of its Controller). for the following purposes: (i) Processing in accordance with the Agreement (s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by ConnectWise 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 Personal Data and the categories of Data Subjects Processed under this DPA are further specified below within Annex I, Section (B) Description of Transfer in this DPA.

3.0 Rights of Data Subjects

3.1 Data Subject Request. ConnectWise shall, to the extent legally permitted, promptly notify Client (who, where Client is a Processor, shall inform its Controller) if ConnectWise receives a request from a Data Subject (governing their personal data) exercising or declaring their (i) right of access; (ii) right to rectification; (iii) restriction of Processing erasure ("right to be forgotten"); (iv) objection to data portability or Processing; and/or (v) right to not to be subject to automated individual decision making (each such request (i)-(v) being a "Data Subject Request"). Taking into account the nature of the Processing, ConnectWise shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's Obligation(s) (or, where Client is a Processor, its Controller) to respond to a Data Subject Request under Applicable Data Protection Laws and Regulations. To the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, ConnectWise shall upon Client's request provide commercially reasonable efforts to assist Client (or, where Client is a Processor, its Controller) in responding to such Data Subject Request to the extent ConnectWise is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from ConnectWise's provision of such assistance.

4.0 ConnectWise Personnel

4.1 Confidentiality. ConnectWise shall ensure that its personnel engaged in the Processing of Personal Data are (i) informed of the confidential nature of the Personal Data; (ii) have received appropriate training on their responsibilities; and (iii) have executed written confidentiality agreements. ConnectWise shall ensure that such confidentiality Obligations survive the termination of the personnel engagement.

4.2 Reliability. ConnectWise shall take commercially reasonable steps to ensure the reliability of any ConnectWise personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. ConnectWise shall ensure that ConnectWise's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5.0 Sub-Processors

5.1 Appointment of Sub-Processors. Client acknowledges and agrees that (i) ConnectWise's Affiliates may be retained as Sub-Processors; and (ii) ConnectWise and ConnectWise's Affiliates respectively may engage third-party Sub-Processors in connection with the provision of the Services. ConnectWise or a ConnectWise Affiliate has entered into a written agreement with each Sub-Processor containing data protection Obligations not less protective than those in the Agreement with respect to the protection of Client Data to the extent applicable to the nature of the Services provided by such Sub-Processor.

5.2 List of Current Sub-Processors and Notification of New Sub-Processors. ConnectWise shall make available to Client the current list of Sub-Processors for theServices identified within ConnectWise's Business Knowledge Document, which it shall update with details of any change in Sub-Processors and notify Client of the same at least ten (10) days' prior to any such change; (ii) ConnectWise imposes data protection terms requiring the protection of Client Data on any Sub-Processor it appoints to the standard required by Applicable Data Protection Laws and Regulations ; and (iii) ConnectWise remains liable for any breach of this DPA that is caused by an act, error or omission of its Sub-Processor. Client (where Client is a Processor, shall reflect the instructions of its Controller) may object to ConnectWise's appointment or replacement of a Sub-Processor prior to its appointment or replacement, provided such objection is reasonable and founded on demonstrable grounds relating to the Sub-Processor's inability to comply with Applicable Data Protection Laws and Regulations. Client shall render their objection to ConnectWise's use of a new Sub-Processor and the applicable Personal Data ("Sub-Processor Objection") promptly in writing to the address and point of contact as defined within the Notice provision contained in the Agreement within thirty (30) days of receipt of ConnectWise's notice. If Client objects to a new Sub-Processor as permitted in the preceding sentence, ConnectWise will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services ("Service Alteration") intended to avoid the Processing of the Personal Data which Client has clearly identified within their Sub-Processor Objection without unreasonably burdening Customer. If ConnectWise is unable to render a Service Alteration within a reasonable period of time, which shall not exceed sixty (60) days from ConnectWise's receipt of Client's Sub-Processor Objection, Client may terminate only those Services contained within the applicable Agreement, which cannot be provided by ConnectWise without the use of the Sub-Processor by providing written notice ("Service Cancellation Notice") to ConnectWise at the address and point of contact as defined within the Notice provision contained in the Agreement, within thirty (30) days of receipt of ConnectWise's notice of its inability to render a Service Alteration. Client's Service Cancellation Notice shall explicitly detail the specific Services they are seeking to terminate under the Agreement. Following ConnectWise's receipt of Client's Service Cancellation Notice, a refund will be issued to Client for any prepaid fees covering the remainder of the term of such specific Services rendered under the Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Client. For the avoidance of doubt, the entirety of the Agreement will not be cancelled following receipt of the Service Cancellation Notice, only the individual Services in which ConnectWise is unable cure through a Service Alteration) to provide an

5.3 Liability. ConnectWise shall be liable for the acts and omissions of its Sub-Processors to the same extent ConnectWise would be liable if performing the services of each Sub-Processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6.0 Security

6.1 Controls for the Protection of Client Data. ConnectWise shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data), confidentiality, and integrity of Client Data, as set forth within its the Technical and Organization Measures Security Documentation. ConnectWise regularly monitors compliance with these measures. ConnectWise will not materially decrease the overall security of the Services during a subscription term.

6.2 Third-Party Certifications and Audits.

6.2.1 ConnectWise has obtained the third-party certifications and audits set forth within its Security, Privacy and Architecture Documentation. Upon Client's written request (and, where Client is a Processor, shall reflect the instructions of its Controller) at reasonable intervals, and subject to the confidentiality Obligations set forth in the Agreement, ConnectWise shall make available to Client (and, where Client is a Processor, its Controller), that is not a competitor of ConnectWise (or Client's independent, third-party auditor that is not a competitor of ConnectWise) a copy of ConnectWise's then most recent third-party audits or certifications, as applicable, and to the extent ConnectWise makes them generally available to its Clients.

6.2.2 Client may contact ConnectWise (providing they render reasonable notice) and request an in-person audit ("On-Site Audit") of the procedures relevant to the protection of Personal Data pursuant to this DPA, provided Client conducts the On-Site Audit during ConnectWise's normal business hours, and takes all reasonable measures to prevent any unnecessary disruption(s) to ConnectWise, and Client does not exercise its right to an On-Site Audit more than once per calendar year. Client shall reimburse ConnectWise for any time expended for an On-Site Audit at the ConnectWise Group's then-current professional services rates, which shall be made available to Client upon request. Before the commencement of an On-Site Audit, the Parties shall mutually agree upon the scope, timing, and duration of the On-Site Audit in addition to the reimbursement rate for which Client shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by ConnectWise. Client shall promptly notify ConnectWise in writing with any findings of non-compliance discovered during the course of the On-Site Audit.

6.3 Data Protection Impact Assessment. Upon Client's request (in instances where Client is a Processor, such request should include the instructions of its Controller), ConnectWise shall provide Client with reasonable cooperation and assistance necessary to fulfill Client's Obligation(s) (or, where Client is a Processor, the Obligation(s) of its Controller) under the Applicable Data Protection Laws and Regulations to carry out a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is reasonably available to ConnectWise.

7.0 Client Data Incident Management and Notification

ConnectWise maintains security incident management policies and procedures as specified within the ConnectWise Trust site, and shall notify Client (who, where Client is a processor, shall in turn inform its Controller) without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data, including Personal Data, transmitted, stored or otherwise Processed by ConnectWise or its Sub-Processors of which ConnectWise becomes aware (a "Client Data Incident"). ConnectWise shall make reasonable efforts to identify the cause of such Client Data Incident and take those steps deemed necessary and reasonable by ConnectWise to remediate the cause of such a Client Data Incident to the extent that the remediation is within ConnectWise's reasonable control. The Obligations herein shall not apply to incidents that are caused by Client, Client's Controller(s), or Client's Users.

8.0 Deletion of Client Data

To the extent allowed by applicable law, ConnectWise shall delete Client Data within sixty (60) days of the receipt of notification from the Client (and, where Client is a Processor, such notification shall reflect the instructions of the Client's Controller).

9.0 Authorized Affiliates

9.1 Contractual Relationship. The Parties acknowledge and agree that, by executing the Agreement, Client enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between ConnectWise and each such Authorized Affiliate subject to the provisions of the Agreement, and Section 9 and Section 10 of this DPA. Each Authorized Affiliate agrees to be bound by the Obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not, and does not, become a party to the Agreement and is only a party to the DPA. All access to, and use of, the Services and content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Client.

9.2 Communication. The Client that is the contracting party to the Agreement shall remain responsible for coordinating all communication with ConnectWise under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with ConnectWise, it shall to the extent required under Applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where Applicable Data Protection Laws and Regulations require the Authorized Affiliate to directly (by itself) exercise a right or seek any remedy under this DPA against ConnectWise, the Parties agree that (i) the Client that is the contracting party to the Agreement shall solely exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Client that is the contracting party to the Agreement shall solely exercise any such rights under this DPA. The Client shall not exercise any remedy separately for each individual Authorized Affiliate individual, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth in Section 9.3.2 of this DPA below, for example).

9.3.2 The Parties agree that Client as the contracting party to the Agreement shall take all reasonable measures to limit any impact on ConnectWise and its Sub-Processors when carrying out an On-Site Audit, by combining, to the extent reasonably possible, all requests for an On-Site Audit sought on behalf of itself and all of its Authorized Affiliates, as well as the subsequent commencement of such On-Site Audit into a singular combined event.

10. 0 Limitation of Liability

The combined aggregate liability of each Party and all of its Affiliates arising out of, or related to this DPA, and all DPAs between Authorized Affiliates and ConnectWise, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs collectively. For the avoidance of doubt, the total liability for ConnectWise and its Affiliates associated with all claims from Client and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Client and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Client and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11.0 European Specific Provisions

11.1 GDPR. ConnectWise will Process Personal Data in accordance with the EU GDPR/ UK GDPR requirements directly applicable to ConnectWise's provision of its Services.

11.2 Data Protection Impact Assessment. ConnectWise shall provide reasonable assistance to Client in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 6.3 of this DPA, to the extent required under the EU GDPR/ UK GDPR.

11.3 Restricted Transfers. The Parties agree that when the transfer of Personal Data from Client to ConnectWise is a Restricted Transfer it shall be subject to the appropriate EU SCC's as follows:

11.3.1 in relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply, completed as follows:

a) Module Two: Transfer Controller to Processor will apply to the extent that Client is a Controller of the Data;

b) Module Three: Transfer Processor to Processor will apply to the extent that Client is a Processor of the Personal Data on behalf of a third-party Controller;

c) Clause 7, *Optional* Docking Clause does not apply;

d) Clause 9, Use of Sub-Processors, Option 2: General Written Authorisation will apply, and the time period for prior notice of sub-processor changes shall be as set forth in Section 5.2 of this DPA;

e) Clause 11, Redress, *Option* the optional language will not apply;

f) Clause 17, Governing Law, Option 1 will apply, and the EU SCCs will be governed by the law(s) of the Republic of Ireland;

g) Any applicable disputes in accordance with Clause 18, Choice of Forum and Jurisdiction, Section (b) shall be resolved before the courts of the Republic of Ireland;

h) Annex I, List of Parties shall be deemed completed with the information set forth in Annex I of this DPA;

i) Annex II Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data shall be deemed completed with the information set out in Annex II to this DPA; and

j) Annex III, List of the Processors shall be deemed completed with the information set out in Annex III to this DPA.

11.3.2 in relation to Sub-Processors Data that is protected by the UK GDPR, the UK Addendum will apply and deemed completed as follows:

a) The EU SCCs, completed as detailed above in Section 11.3.1 of this DPA shall also apply to transfers of such Personal Data, subject to Section 11.3.2(b) of this DPA as provided below;

b) Under the UK Addendum, Part 1: Tables, the following shall be deemed completed with the relevant information provided above as set forth within the EU SCCs: (i) Table: 1 Parties; (ii) Table 2: Selected SCCs, Models and Selected Clauses, and (iii) Table 3: Appendix information.

c) The start date of the UK Addendum as set forth in Part 1: Tables, Table: 1 Parties, shall be identified as the date of this DPA.

d) Table 4: Ending this Addendum When Approved Addendum Changes, as contained within Part 1: Tables of the UK Addendum shall be deemed completed with the selection of the option of "neither Party".

11.3.3 in the event that any provision of this Agreement contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11.4 Transfer Mechanisms for Data Transfers. Subject to the additional terms set forth below in Schedule 1 of this DPA, ConnectWise incorporates the EU SCCs as detailed within Section 11.3 of this DPA and:

11.4.1 When Client is acting as a processor, the applicable Processor-to-Processor Clauses within the EU SCCs will apply to a Restricted Transfer. Taking into account the nature of the processing, Client agrees that it is unlikely that ConnectWise will know the identity of Client's Controllers as ConnectWise does not have a direct relationship with Client's Controllers and therefore, Client will fulfill ConnectWise's Obligations to Client's Controllers under the Processor-to-Processor Clauses.

12.0 Legal Effect

This DPA shall only become legally binding between the Parties when the formalities and steps set out in this DPA have been fully completed.

SCHEDULE(S)/ ANNEX(ES)

I. Schedule 1: Additional Terms for Restricted Transfers

II. Annexes to Standard Contractual Clauses:

a. Annex I: List of Parties and Description/Categories of Transfer
b. Annex II: Technical and Organisational Measures
c. Annex III: List of Sub-Processors

SCHEDULE 1

1.0 Additional Terms for Restricted Transfers

1.1. Clients Covered by Standard Contractual Clauses. The SCCs and the additional terms specified within this Schedule 1, apply to (i) any Client which is subject to the SCCs to the extent relevant under Applicable Data Protection Laws and Regulations (and shall therefore be taken to be a Restricted Transfer) and its Authorized Affiliates as applicable. For the purpose of the SCCs and Schedule 1, of this DPA, the Client and its Affiliates shall be deemed "Data Exporters".

1.2. Certification of Deletion. The Parties agree that the certification of deletion of Personal Data that is described within Clause 16, Non-Compliance with the Clauses and Termination, Section (d) of the SCC shall be provided by ConnectWise to Client only upon Client's request (where Client is a Processor, such request shall reflect the instructions of its Controller).

1.3. Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the SCC) and the SCC, the SCC shall prevail.

ANNEX I

A. List of Parties

1. Data Exporter(s): The name and accompanying contact details for the for the Data Exporter and, where applicable, of its Data Protection Officer and/or designated representative within the European Union are as follows:

   Name: ***The Client as identified within the Agreement.***

   Address: ***Client's address as specified within the Agreement.***

   Name of Designated Point of Contact: ***The Client's designated contact shall be the individual identified as "Client's Primary Contact" within the Agreement (including name, position, and corresponding contact details).***

   Activities Relevant to the Data Transferred Under the SCC: ***The relevant activities subject to the regulation of the SCC encompass the provision of software and related services by ConnectWise to Client.***

   Role: Controller/ (Processor, as applicable).

2. Data Importer(s): The name and accompanying contact details for the for the Data Importer and, where applicable, of its Data Protection Officer and/or designated representative within the European Union are as follows:

   a) Name: ***ConnectWise, LLC***

   b) Address: ***400 N. Tampa Street, Suite 130, Tampa, Florida 33602***

   c) Name of Designated Point of Contact: ***Contact with ConnectWise shall be initiated at Privacy@ConnectWise.com. Supplemental contact information and notice procedures for ConnectWise are identified within the Agreement.***

   d) Activities Relevant to the Data Transferred Under the SCC: ***The relevant activities subject to the regulation of the SCC encompass the provision of software and related services by ConnectWise to Client.***

   e) Role: ***Processor.***

B. Description of Transfer

1. Data Subjects. The categories of Data Subjects whose Personal Data is transferred include the following:

   a) ***Client's Employees; and***

b) ***Client's Contractors.***

Additionally, Client may submit Personal Data to the Services, to the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

c) ***Prospects, Customers, Business Partners and Vendors of Client (who are natural persons);***

d) ***Employees or Contact persons of Client's Prospects, Customers, Business Partners and Vendors;***

e) ***Employees, Agents, Advisors, Freelancers of Client (who are natural persons); and***

f) ***Client's Users authorized by Client to use the Services.***

2. Personal Data. The categories of Personal Data that are being transferred include the following:

a) ***First and Last Name;***

b) ***Contact Information;***

- ***i. Company name***
- ***ii. Email Address***
- ***iii. Phone Number***
- ***iv. Physical Business Address***

c) ***Position;***

d) ***Employer;***

e) ***Mailing Address;***

f) ***Business Phone;***

g) ***Mobile Phone;***

h) ***Computer Name;***

i) ***Computer IP Address;***

j) ***Computer MAC Address;***

k) ***Computer Access Password;***

l) ***ID Data;***

m) ***Professional Life Data;***

n) ***Connection Data;***

o) ***Localisation Data;***

The collection of Client's Computer Name, IP address, and Mac Address by ConnectWise are a result of the installation and utilization of the Offering on Client's endpoints.

In addition, ConnectWise may process, under the terms of the Agreement, personal data which the end-client elects to host with or *upload to the Client in connection with the Client's provision of Services to its end-client.*

3. Sensitive Data Transferred and Applied Safeguards. Identify any sensitive date transferred (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 as follows:

a) The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Continuous.

b) Nature of the processing.

ConnectWise will Process Personal Data as necessary to perform the Services pursuant to the Agreement, in accordance with Section 2.0 of this DPA, and as further instructed by Client in its use of the Services.

c) Purpose(s) of the data transfer and further processing.

ConnectWise will Process Personal Data as necessary to perform the Services pursuant to the Agreement, in accordance with Section 2.0 of this DPA, and as further instructed by Client in its use of the Services.

d) The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

ConnectWise will retain Personal Data as necessary to perform the Services pursuant to the Agreement, in accordance with Section 8.0 of this DPA, and as further instructed by Client in its use of the Services.

e) For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

ConnectWise will transfer to sub-processors as necessary to perform the Services pursuant to the Agreement, in accordance with its Technical and Organization Measures Security Documentation, and as further instructed by Client in its use of the Services.

C. Competent Supervisory Authority

1. Supervisory Authority. Identify the competent supervisory authority/ies in accordance with Clause 13 [of the SCC].

The supervisory authority will be rendered in accordance with the directives set forth in Clause 13 of the SCC.

ANNEX II

A. Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

1. Measures of pseudonymization and encryption of personal data.

   ConnectWise maintains Client Data in an encrypted format at rest using Advanced Encryption Standard and in transit using TLS.

2. Measures for ensuring ongoing confidentiality, integrity, and availability and resilience of processing systems and services.

   ConnectWise's customer agreements contain strict confidentiality obligations. Additionally, ConnectWise requires every downstream Sub-processor to sign confidentiality provisions that are substantially similar to those contained in ConnectWise's customer agreements. The infrastructure for ConnectWise Offerings spans multiple cloud environments utilizing fault-independent availability zones in geographic regions physically separated from one another, supported by various tools and processes to maintain high availability of services.

3. Measures for ensuring the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

   ConnectWise performs regular data backups of Client Data, which is hosted in AWS and various cloud data centers. Backups are retained redundantly across multiple availability zones and encrypted in transit and at rest using Advanced Encryption Standard (AES-256).

4. Processes for regular testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing.

   ConnectWise maintains a risk-based assessment security program. The framework for ConnectWise's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Offerings and confidentiality, integrity, and availability of Client Data. ConnectWise's security program is intended to be appropriate to the nature of the Offerings and the size and complexity of ConnectWise's business operations. ConnectWise has a separate and dedicated security team that manages ConnectWise's security program. This team facilitates and supports independent audits and assessments performed by third-parties to provide independent feedback on the operating effectiveness of the information security program.

5. Measures for user identification and authorization.

   ConnectWise personnel are required to use unique user access credentials and passwords for authorization. ConnectWise follows the principles of least privilege through role-based and time-based access models when provisioning system access.

ConnectWise personnel are authorized to access Client Data based on their job function, role and responsibilities, and such access requires approval prior to access provisioning. Access is promptly removed upon role change or termination.

6. Measures for the protection of data during transmission.

    End customer Data is encrypted when in transit between Customer and the corresponding ConnectWise Offering using TLS.

7. Measures for the protection of data during storage.

    Client Data is stored encrypted using the Advanced Encryption Standard.

8. Measures for ensuring physical security of locations at which personal data are processed.

    ConnectWise headquarters and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security. All employees, contractors, and visitors are required to wear identification badges.

    The Offerings operate on Amazon Web Offerings ("AWS") and other cloud providers listed on the ConnectWise Sub-Processor list and are protected by the security and environmental controls of respective cloud provider.

9. Measures for ensuring events logging.

    ConnectWise monitors access to applications, tools, and resources that process or store Client Data, including cloud services. Monitoring of security logs is centralized by the security team. Log activities are investigated when necessary and escalated appropriately.

10. Measures for ensuring systems configuration, including default configuration.

    ConnectWise applies Secure Software Development Lifecycle (Secure SDLC) standards to perform numerous security-related activities for the Offerings across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before new Offerings are deployed; (b) annual penetration testing by independent third parties; and (c) threat models for new Offerings to detect any potential security threats and vulnerabilities.

    ConnectWise adheres to a change management process to administer changes to the production environment for the

Offerings, including changes to its underlying software, applications, and systems.

11. Measures for internal IT and IT security governance and management.

ConnectWise maintains a risk-based assessment security program. The framework for ConnectWise's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Offerings and confidentiality, integrity, and availability of Client Data. ConnectWise's security program is intended to be appropriate to the nature of the Offerings and the size and complexity of ConnectWise's business operations. ConnectWise has a separate and dedicated Information Security team that manages ConnectWise's security program. This team facilitates and supports independent audits and assessments performed by third parties. ConnectWise's security framework is based on the ISO 27001 Information Security Management System and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response. Security is managed at the highest levels of the company, with the Chief Information Security Officer meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all ConnectWise employees for their reference.

12. Measures for certifications/assurance of processes and products.

ConnectWise conducts various third-party audits to attest to various frameworks including SOC 2 Type 2, and annual application penetration testing.

13. Measures for ensuring data minimization.

ConnectWise Customers unilaterally determine what Client Data they store and consume within the ConnectWise Offerings and how the Offerings are configured. As such, ConnectWise operates on a shared responsibility model. ConnectWise provides tools within the Offerings that gives Customers control over exactly what data enters the platform and enables Customers with the ability to block data at the Source level. Additionally, ConnectWise has built in self-service functionality to the Offerings that allow Customers to delete and suppress Client Data on demand.

14. Measures for ensuring data quality.

ConnectWise has a multi-fold approach for ensuring data quality. These measures include: (i) unit testing to ensure the quality of logic used to make API calls, and (ii) volume testing to ensure the

code is able to scale. ConnectWise applies these measures across the board, both to ensure the quality of any Usage Data that ConnectWise collects and to ensure that the ConnectWise Platform is operating in accordance with the documentation.

Each ConnectWise Partner chooses what Client Data they route through the ConnectWise Offerings and how the Offerings are configured. As such, ConnectWise operates on a shared responsibility model. ConnectWise ensures that data quality is maintained from the time a Customer sends Client Data into the Offerings and while maintained within the Offerings.

15. Measures for ensuring limited data retention.

ConnectWise Customers unilaterally determine what Client Data they route through the ConnectWise Offerings and how the Offerings are configured. As such, ConnectWise operates on a shared responsibility model. If a Partner is unable to delete Client Data via the functionality within the Offering, then ConnectWise deletes Client Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law.

16. Measures for ensuring accountability.

ConnectWise has adopted measures for ensuring accountability, such as implementing data protection policies across the business, maintaining documentation of processing activities, recording and reporting Security Incidents involving Personal Data. Additionally, ConnectWise conducts regular third-party audits to ensure compliance with our privacy and security standards.

17. Measures for allowing data portability and ensuring erasure.

ConnectWise's Partners have direct relationships with their end customers and are responsible for responding to requests from their end customers who wish to exercise their rights under Applicable Data Protection Laws. If ConnectWise receives a request from a Data Subject in relation to their Client Data, ConnectWise will advise the Data Subject to submit their request to the Partner, and the Partner will be responsible for responding to any such request.

ANNEX III

A. List of Sub-Processors

1. Sub-Processors: Provide the list of sub-processors utilized.

   The list of Sub-Processors utilized by ConnectWise is published and available under the List of ConnectWise Sub-Processors section of the ConnectWise.com website.