Release Date: Version 2.0, October 16, 2023

Limble Data Processing Addendum

This Data Processing Addendum ("**Addendum**") completes and forms part of the Terms of Service, as updated from time to time, or other agreement between Limble and Customer (together the "**Parties**") governing Customer's use of the Service (altogether "**Principal Agreement**"). This Addendum is concluded between Limble Solutions, Inc., and its affiliates, subsidiaries and branches ("**Limble**") and the Customer as defined in the Principal Agreement ("**Customer**").

The Parties agree that the terms set out below are added as an Addendum to the Principal Agreement.

1. **Definitions and Interpretation**

1.1. In this Addendum:

1.1.1. **"Applicable Data Protection Law"** means the following data protection law(s), as applicable, including any subsequent amendments, modifications and revisions thereto: (i) European Data Protection Law, including the GDPR; and (ii) the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 ("**CCPA**") and any other applicable U.S. federal and state privacy laws that apply generally to the processing of individuals' Personal Data and that do not apply solely to specific industry sectors (e.g., financial institutions), specific demographics (e.g., children), or specific classes of information (e.g., health or biometric information) (**"U.S. Privacy Laws**");

1.1.2. "**Consumer**" has the meaning defined in the U.S. Privacy Laws;

1.1.3. "**Customer Personal Data**" means Personal Data Processed by Limble as a Processor on behalf of Customer or Third Party Controller;

1.1.4. "**Data Subject Rights**" means Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, the right to withdraw consent, and the right not to be subject to automated individual decision-making in accordance with Applicable Data Protection Law;

1.1.5. "**European Data Protection Law**" means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), their national implementations in the European Economic Area ("**EEA**"), including the European Union, and all other data protection laws of the EEA, the United Kingdom ("**UK**"), and Switzerland, each as applicable, and as may be amended or replaced from time to time;

1.1.6. "**International Data Transfer**" means any disclosure of Customer Personal Data by an organization subject to European Data Protection Law to another organization located outside the EEA, the UK, or Switzerland;

1.1.7. "**Services**" means the services provided by Limble to Customer as defined in Section 1.2.6 of the Principal Agreement;

1.1.8. "**Share**," "**Shared**," and "**Sharing**" have the meaning defined in the CCPA;

1.1.9. "**Sale**" and "**Selling**" have the meaning defined in the U.S. Privacy Laws;

1.1.10. "**Subprocessor**" means a Processor engaged by Limble to Process Customer Personal Data;

1.1.11. "**SCCs**" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 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 as amended or replaced from time to time;

1.1.12. "**Third-Party Controller**" means a Controller for which Customer is a Processor;

1.1.13. "**UK Addendum**" means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022); and

1.1.14. "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", "**Processed**" and "**Supervisory Authority**" have the meaning given to them in Applicable Data Protection Law, and their cognate terms shall be construed accordingly.

1.1.15. In the event of a conflict in the meanings of defined terms in the U.S. Privacy Laws, the meaning from the law applicable to the state of residence of the relevant Consumer applies.

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Principal Agreement.

2. **Scope**

2.1. This Addendum applies to the Processing of Customer Personal Data by Limble subject to Applicable Data Protection Law to provide the Services.

2.2. The subject matter, nature, and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects are set out in **Annex I**, which is an integral part of this Addendum.

2.3. Customer is a Controller and appoints Limble as a Processor on behalf of Customer. Limble will only Process Customer Personal Data on behalf of Customer for the limited and specific purposes set forth in **Annex I**. Customer is responsible for compliance with the requirements of Applicable Data Protection Law applicable to Controllers.

2.4. If Customer is a Processor on behalf of a Third-Party Controller, then Customer: is the single point of contact for Limble; must obtain all necessary authorizations from such Third-Party Controller; and undertakes to issue all instructions and exercise all rights on behalf of such other Third-Party Controller.

2.5. Customer acknowledges that Limble may Process Personal Data relating to the operation,

support, or use of the Services for its own business purposes, such as accounting and finance, account management, data analysis, benchmarking, product development, sales and marketing, and compliance with law, and including as described in Section 8.3 of the Principal Agreement. Limble is the Controller for such Processing and will Process such data in accordance with Applicable Data Protection Law.

3. **Processing of Customer Personal Data**

3.1. Limble shall:

3.1.1. comply with Applicable Data Protection Laws in the Processing of Customer Personal Data, provide the level of privacy protection required by the U.S. Privacy Laws and provide Customer with all reasonably-requested assistance to enable Customer to fulfill its own obligations under the U.S. Privacy Laws;

3.1.2. not Process Customer Personal Data other than on the Customer's documented instructions; and

3.1.3. With respect to the Processing of Personal Data subject to U.S. Privacy Laws, except as explicitly permitted by the applicable U.S. Privacy Laws, Limble is prohibited from (i) Selling or Sharing Customer Personal Data, (ii) retaining, using, or disclosing Customer Personal Data for any purpose other than for the specific purpose of performing the services specified in Annex I, (iii) retaining, using, or disclosing Customer Personal Data outside of the direct business relationship between the Parties, and (iv) combining Customer Personal Data with Personal Data obtained from, or on behalf of, sources other than Customer.

3.2. Customer hereby instructs Limble to process Customer Personal Data to provide the Services in accordance with the Principal Agreement and this Addendum, or any applicable statement of work.

3.3. Customer may reasonably issue additional instructions as necessary to comply with Applicable Data Protection Law.

3.4. Unless prohibited by applicable law, Limble will inform Customer if Limble is subject to a legal obligation that requires Limble to Process Customer Personal Data in contravention of Customer's documented instructions.

4. **Processor Personnel**

4.1. Limble will ensure that all personnel including employees, agents, sub-contractors and sub-processors authorized to Process Customer Personal Data are subject to an obligation of confidentiality.

5. **Security**

5.1. 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, Limble shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the

measures described in **Annex II**.

5.2. Customer acknowledges that the security measures in Annex II are appropriate in relation to the risks associated with Customer's intended Processing and will notify Limble prior to any intended Processing for which Limble's security measures may not be appropriate.

6. **Subprocessing**

6.1. Customer hereby authorizes Limble to engage Subprocessors. A list of Limble's current Subprocessors is included in https://trust.limblecmms.com/.

6.2. Limble will enter into a written agreement with Subprocessors which imposes the same obligations as required by Applicable Data Protection Law. Limble shall specifically ensure that Limble's subcontractors or Subprocessors who Process Customer Personal Data on Limble's behalf agree in writing to the same or equivalent restrictions and requirements that apply to Limble in this Addendum and the Principal Agreement with respect to Customer Personal Data, as well as to comply with the applicable U.S. Privacy Laws.

6.3. Limble will notify Customer prior to any intended change to Subprocessors. Customer may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Applicable Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Limble's notification of the intended change. Customer and Limble will work together in good faith to address Customer's objection. If Limble chooses to retain the Subprocessor, Limble will inform Customer at least thirty (30) days before authorizing the Subprocessor to Process Customer Personal Data, and either party may immediately discontinue providing or using the relevant parts of the Services, as applicable, and may terminate the relevant parts of the Services within thirty (30) days.

6.4. If any Subprocessor fails to fulfill its obligations under Applicable Data Protection Law, Limble will be fully liable to Customer for the performance of such obligations.

7. **Data Subject Rights and Consumer Rights**

7.1. Limble shall promptly notify Customer if it determines that it can no longer meet its obligations under applicable U.S. Privacy Laws. Upon receiving notice from Limble in accordance with this subsection, Customer may direct Limble to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

7.2. Taking into account the nature of the Processing, Limble shall provide commercially reasonable assistance to the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligations to respond to requests to exercise Data Subject Rights and U.S. Privacy Law-related Consumer rights requests under the Applicable Data Protection Laws.

7.3. Limble shall:

7.3.1. promptly notify Customer if it receives a request to exercise Data Subject Rights under Applicable Data Protection Law in respect of Customer Personal Data; and

7.3.2. ensure that it does not respond to that request except on the documented

instructions of Customer or as required by applicable law to which Limble is subject, in which case Limble shall to the extent permitted by applicable law inform Customer of that legal requirement before Limble responds to the request.

7.4. Customer shall promptly inform Limble if it receives any request to exercise Data Subject Rights or any Consumer request made pursuant to the U.S. Privacy Laws affecting Customer Personal Data Processed by Limble that Customer must comply with. Customer shall provide Limble with the information necessary for Limble to comply with any such request.

7.5. Limble shall not be required to delete any Customer Personal Data to comply with a Consumer's request directed by Customer if retaining such information is specifically permitted by applicable U.S. Privacy Laws; provided, however, that in such case, Limble will promptly inform Customer of the exceptions relied upon under applicable U.S. Privacy Laws and Limble shall not use Customer Personal Data retained for any purpose other than provided for by that exception.

8. **Personal Data Breach**

8.1. Limble will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data. If Limble's notification is delayed, it will be accompanied by reasons for the delay.

8.2. Limble shall take reasonable commercial steps in the investigation, mitigation and remediation of a Personal Data Breach affecting Customer Personal Data.

8.3. Limble shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligations under European Data Protection Law to notify Personal Data Breaches to Supervisory Authorities and Data Subjects, as applicable.

9. **Data Protection Impact Assessment and Prior Consultation**

9.1. Taking into account the nature of the Processing, Limble shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligations under European Data Protection Law to conduct data protection impact assessments, and prior consultations with Supervisory Authorities, as applicable.

10. **Audit**

10.1. Upon reasonable request, Limble must make available to Customer all information necessary to demonstrate compliance with the obligations of this Addendum and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested no more than once per year by Customer, and performed by an independent auditor as agreed upon by Customer and Limble. The foregoing shall only extend to those documents and facilities relevant and material to the Processing of Customer Personal Data and shall be conducted during normal business hours and in a manner that causes minimal disruption. Limble and Customer each bear

their own costs related to an audit.

10.2. With respect to the Processing of Personal Data subject to U.S. Privacy Laws, Customer has the right to monitor Limble's compliance with this Addendum through measures, including, but not limited to, ongoing manual reviews, automated scans, regular assessments, audits, or other annual technical and operational testing at least once every 12 months

10.3. Where permitted by law, Limble may instead make available to Customer a summary of the results of a third-party audit or certification reports relevant to Limble's compliance with this Addendum.

11. **International Data Transfers**

11.1. Customer hereby authorizes Limble to perform International Data Transfers to any country deemed to have an adequate level of data protection by the European Commission or other competent authorities (including the competent authorities in the UK and Switzerland), as appropriate; on the basis of adequate safeguards in accordance with European Data Protection Law; or pursuant to the SCCs and the UK Addendum referred to in Sections 11.2 and 11.3.

11.2. By signing this Addendum, Customer and Limble conclude Module 2 (controller-to-processor) of the SCCs and, to the extent Customer is a Processor on behalf of a Third-Party Controller, Module 3 (Processor-to-Subprocessor) of the SCCs, which are hereby incorporated and completed as follows: the "data exporter" is Customer; the "data importer" is Limble; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented and the time period therein is specified in Section 6.3 above; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland; the courts in Clause 18(b) are the Courts of Ireland; Annex I and II to Module 2 and 3 of the SCCs are **Annex I and II** to this Addendum respectively. For International Data Transfers from Switzerland, Data Subjects who have their habitual residence in Switzerland may bring claims under the SCCs before the courts of Switzerland.

11.3. By signing this Addendum, Limble and Customer conclude the UK Addendum, which is hereby incorporated and applies to International Data Transfers outside the UK. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Customer and the "Importer" is Limble, their details are set forth in the signature block below; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in Section 11.2 of this Addendum; (iii) in Table 3, Annexes 1 (A and B) and II to the "Approved EU SCCs" are **Annex I and II** respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

11.4. If Limble's compliance with European Data Protection Law applicable to International Data Transfers is affected by circumstances outside of Limble's control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Customer and Limble will work together in good faith to reasonably resolve such non-compliance. In the event that additional, replacement or alternative standard contractual clauses or UK standard contractual clauses are approved by Supervisory Authorities or other competent authorities, Limble reserves the right to amend this Addendum by

adding to or replacing, the standard contractual clauses or UK standard contractual clauses that form part of it at the date of signature in order to ensure continued compliance with European Data Protection Law.

12. Liability

12.1. Without prejudice to Section 9.2 of the Principal Agreement, where Limble has paid compensation, damages or fines, Limble is entitled to claim back from Customer that part of the compensation, damages or fines, corresponding to Customer's part of responsibility for the compensation, damages or fines.

13. Termination and return or deletion

13.1. This Addendum is terminated upon the termination of the Principal Agreement.

13.2. Customer may request return of Customer Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Limble will delete all remaining copies of Customer Personal Data after returning Customer Personal Data to Customer.

14. Applicable law and jurisdiction

14.1. This Addendum is governed by the laws of the State of Utah. Any disputes relating to this Addendum will be subject to the exclusive jurisdiction of the courts of Salt Lake City or Country, in the State of Utah.

15. Modification of this Addendum

15.1. This Addendum may only be modified by a written amendment signed by both Limble and Customer.

16. Invalidity and severability

16.1. If any provision of this Addendum is found by any court or administrative body of a competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this Addendum and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

ANNEX I
DESCRIPTION OF THE TRANSFER

A. LIST OF PARTIES

Data exporter:

- **Name**: Customer (as defined in the Principal Agreement, and as indicated in the Order Form or the customer's Subscription Software account)
- **Address**: As indicated in the Order Form or in the customer's Subscription Software account.
- **Contact person's name, position and contact details**: As indicated in the Order Form or in the Customer's Subscription Software account.
- **Activities relevant to the data transferred under these Clauses**: Customer receives Limble's Services as described in the Principal Agreement and Customer provides Personal Data to Limble in that context.
- **Signature and date**: See the Order Form or the electronic acceptance of the Principal Agreement through the Subscription Software's self-serve subscription tool.
- **Role (controller/processor)**: Controller, or Processor on behalf of Third-Party Controller

Data importer:

- **Name**: Limble Solutions, Inc.
- **Address**: 3290 West Mayflower Way, Lehi, UT 84043, United States of America.
- **Contact person's name, position and contact details**: Caleb Frischknecht, General Counsel, legal@limblecmms.com,Tel: 801-851-1218.
- **Activities relevant to the data transferred under these Clauses**: Limble provides its Services to Customer as described in the Principal Agreement and Processes Personal Data on behalf of Customer in that context.
- **Signature and date**: See the Order Form or the electronic acceptance of the Principal Agreement through the Subscription Software's self-serve subscription tool
- **Role (controller/processor)**: Processor on behalf of Customer, or Subprocessor on behalf of Third-Party Controller

B. DESCRIPTION OF INTERNATIONAL DATA TRANSFER

- **Categories of Data Subjects whose Personal Data is transferred**: Customer's personnel, staff, contractors and consultants; and any other "Authorized Users" as defined in the Principal Agreement.

- **Categories of Personal Data transferred**:

#	Category of Personal Data
1.	Account details, such as given name, last name, username, and password, and account information on third-party services which the Customer chooses to integrate with the Services.

2.	Professional contact details, such as company name, job title, email address, phone numbers, fax number, physical address, fees for completing maintenance tasks.
3.	User content, such as information about ongoing and completed work orders and projects, project deadlines and status, inventory of available tools and technology, images showing maintenance needs and project status, location of projects, chat messages between users, and any other content uploaded by users of Limble's Services.
4.	Support information, such as information included in technical support requests sent by Customer, any additional information provided by Customer, and information about the type of technical support provided to Customer.
5.	Communications, such as contact details (e.g., name, email address, postal address, telephone number) and the contents of any message sent to Limble's customer support and customer management teams.

- **Sensitive data 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**: Limble does not intend to receive sensitive Personal Data from its Customers.
- **The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)**: On a continuous basis for the duration of the Principal Agreement.
- **Nature of the processing**: The Personal Data will be processed and transferred as described in the Principal Agreement.
- **Purpose(s) of the data transfer and further processing**: The Personal Data will be transferred and further processed for the provision of the Services as described in the Principal Agreement.
- **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**: Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Applicable Data Protection Law.
- **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**: For the subject matter and nature of the Processing, reference is made to the Principal Agreement and this Addendum. The Processing will take place for the duration of the Principal Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

- The competent authority for the Processing of Personal Data relating to Data Subjects located in the EEA is the Supervisory Authority: (a) of Customer's country of establishment in the EU, or, where not applicable; (b) of the country where the Customer's EU data protection representative is located; or, where not applicable, (c) the Irish Data Protection Commission.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in the UK is the UK Information Commissioner.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in Switzerland is the Swiss Federal Data Protection and Information Commissioner.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Limble Solutions maintains a comprehensive documented security program based on industry best practices and standards, under which Limble Solutions implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Service and personal data (the "**Security Program**"), including, but not limited to, as set forth below. Limble Solutions regularly tests and evaluates its Security Program, and may review and update its Security Program, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

1. Limble Solutions Audits & Certifications

1.1. The information security management system used to provide the service shall be assessed by independent third-party auditors as described in the following audits and certifications ("**Third-Party Audits**"), on at least an annual basis:

- SOC 2 Type II

1.2. To the extent Limble Solutions decides to discontinue a Third-Party Audit, Limble Solutions will adopt or maintain an equivalent, industry-recognized framework.

2. Hosting Location of Personal data

2.1. Hosting Location. The hosting location of personal data is the production Cloud Environment in the Region offered by Limble Solutions and selected by Customer.

3. Encryption

3.1. Encryption of Personal data. Limble Solutions encrypts personal data at-rest using AES 256-bit (or better) encryption, with the exception of object storage, they are protected with object key signing. Limble Solutions uses Transport Layer Security (TLS) 1.2 (or better) for personal data in-transit over untrusted networks.

3.2. Encryption Key Management. Limble Solutions logically separates encryption keys from personal data.

4. System & Network Security

4.1. Access Controls.

4.1.1. All Limble Solutions personnel access to the Cloud Environment is via a unique user ID, consistent with the principle of least privilege, requires a VPN, as well as multi-factor authentication and passwords meeting or exceeding PCI-DSS length and complexity requirements.

4.1.2. Limble Solutions personnel will not access personal data except (i) as reasonably necessary to provide Limble Solutions Offerings under the Principal Agreement or (ii) to comply with the law or a binding order of a governmental body.

4.2. Endpoint Controls. For access to the Cloud Environment, Limble Solutions personnel use Limble Solutions-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

4.3. Separation of Environments. Limble Solutions logically separates production environments from development environments. The Cloud Environment is both logically and physically separate from Limble Solutions' corporate offices and networks.

4.4. Firewalls / Security Groups. Limble Solutions shall protect the Cloud Environment using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required.

4.5. Hardening. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Annex II.

4.6. Monitoring & Logging.

4.6.1. Infrastructure Logs. Monitoring tools or services, such as intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year.

4.7. Vulnerability Detection & Management.

4.7.1. Anti-Virus & Vulnerability Detection. The Cloud Environment leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities. Limble Solutions does not monitor personal data for Malicious Code.

4.7.2. Penetration Testing & Vulnerability Detection. Limble Solutions regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the service at least annually. Limble Solutions also runs vulnerability scans for the Cloud Environment using updated vulnerability databases at least quarterly.

4.7.3. Secure Code Scanning / Review. Limble Solutions has put in place automated code vulnerability assessment tools to assess the potential impact of new code prior to it going into a production environment.

4.7.4. Secure Code Training. Limble Solutions has put into place a policy of at least yearly secure code training for every engineer in the organization.

4.7.5. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the service. Upon becoming aware of such vulnerabilities, Limble Solutions will use commercially reasonable efforts to address private and public (e.g., U.S.-Cert announced) critical and high vulnerabilities within 30 days, and medium vulnerabilities within 90 days. To assess whether a vulnerability is 'critical', 'high', or 'medium', Limble Solutions leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

5. Administrative Controls

5.1. Personnel Security. Limble Solutions requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by applicable law.

5.2. Personnel Training. Limble Solutions maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training at least yearly.

5.3. Personnel Agreements. Limble Solutions personnel are required to sign confidentiality agreements. Limble Solutions personnel are also required to sign Limble Solutions' information security policy, which includes acknowledging responsibility for reporting security incidents.

5.4. Personnel Access Reviews & Separation. Limble Solutions reviews the access privileges of its personnel to the Cloud Environment at least quarterly and removes access on a timely basis for all separated personnel.

5.5. Limble Solutions Risk Management & Threat Assessment. Limble Solutions' risk management process is modeled on SOC 2 Type 2. Limble Solutions' security committee meets regularly to review reports and material changes in the threat environment, and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

5.6. External Threat Intelligence Monitoring. Limble Solutions reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 4.7.3 (Vulnerability Management).

5.7. Change Management. Limble Solutions maintains a documented change management program for the service.

5.8. Vendor Risk Management. Limble Solutions maintains a vendor risk management program for subprocessors that process personal data designed to ensure each subprocessor maintains security measures consistent with Limble Solutions' obligations in this Annex II.

6. Physical & Environmental Controls

6.1. Cloud Environment Data Centers. To ensure the Cloud Provider has appropriate physical and environmental controls for its data centers hosting the Cloud Environment, Limble Solutions regularly reviews those controls as audited under the Cloud Provider's third-party audits and certifications. Each Cloud Provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

6.1.1. Physical access to the facilities are controlled at building ingress points;

6.1.2. Visitors are required to present ID and are signed in;

6.1.3. Physical access to servers is managed by access control devices;

6.1.4. Physical access privileges are reviewed regularly;

6.1.5. Facilities utilize monitor and alarm response procedures;

6.1.6. Use of CCTV;

6.1.7. Fire detection and protection systems;

6.1.8. Power back-up and redundancy systems; and

6.1.9. Climate control systems.

7. Data Backups & Disaster Recovery.

Limble Solutions backs up personal data a minimum of hourly, these backups are automatically replicated to a geographically separate data center inside the same country the data originated, where possible. Backups are replicated at least two different ways offsite to ensure delivery and integrity of the backup. Backups are tested daily by automated processes and the Limble Solutions DevOps team is notified if tests fail to restore personal data. Limble maintains an expected RTO of 24 hours and a RPO of 3 hours. Limble Solutions maintains a disaster recovery plan that is tested yearly for validity, any issues found in the disaster recovery plan are addressed immediately and documented.