Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

DATA PROCESSING ADDENDUM

This Data Processing Addendum **("DPA")** is made on 09-June-26.

Between:

(1) The Healing Link incorporated and registered in United Kingdom whose registered office is at Unit 6, Washington Road,Westbury,Wiltshire,gb,BA13 4JP (the "**Customer"**).

(2) **Zoho Corporation Limited** whose registered office is at Suite B, 3rd Floor, Cbx Ii East, 414-432 Midsummer Boulevard, Milton Keynes, Buckinghamshire, United Kingdom, MK9 2EA ("**Zoho**").

(each a **party** and together the **parties**).

Background:

1. The Customer and Zoho have entered into an agreement for the provision of services under the online terms of service or other electronically/physically signed service agreement (the appropriate one, hereinafter "**Service Agreement**").

2. In the course of providing the services under the Service Agreement, Zoho may, on behalf of the Customer process Personal Data, in connection with the services.

3. Accordingly, parties are entering into this DPA in order to comply with Applicable Data Protection Laws and other legal commitments.

The parties agree as follows:

1. Interpretation

1.1 In this **DPA**:

"**Applicable Data Protection Laws**" means all laws and regulations in the United Kingdom that apply from time to time to data Processing activities by any of the parties, including, but not limited to the Data Protection Act 2018 (UK) and the General Data Protection Regulation;

"**Personal Data**", "**Process**"/"**Processing**", "**Data Controller**", "**Data Processor**", "**Sub-Processor"** and "**Data Subject**" shall have the same meanings as in Applicable Data Protection Laws**.**

"**Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

1.2 This DPA is supplementary to the Service Agreement. The scope of this DPA is strictly limited to the provisions around the Processing of Personal Data as part of the services provided under

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

the Service Agreement and shall not otherwise amend or supersede any rights or obligations of the parties to the Service Agreement.

2. Details of the Processing

The details of the Processing and in particular the special categories of Personal Data, where applicable, are specified in **Appendix 1** which forms an integral part of the DPA.

3. Instructions:

Zoho agrees to process the Personal Data only on behalf of the Customer and in compliance with its instructions. However, Customer agrees that its instructions to Zoho for Processing Personal Data are (i) to Process such data strictly in accordance with the Service Agreement; (ii) to process data where such Processing is initiated by Customer via the user interface of the services; (iii) to process data for fraud prevention, spam filtering, and service improvement, including automation; and (iv) to Process data to comply with other documented reasonable instructions provided by Customer (eg., via email) where such instructions are consistent with the Service Agreement and this DPA. Zoho shall not be obliged to act in accordance with any instructions outside the scope of the Service Agreement except with the prior written agreement of both parties.

4. Documentation and Compliance:

4.1 Demonstration of Compliance. Upon request by Customer, Zoho will demonstrate its compliance with Applicable Data Protection Laws and this DPA by way of reports of audits conducted in the previous 12 months by qualified and independent third party auditors, certifications approved under Article 42 of the UK GDPR, or approved code(s) of conduct as specified under the Applicable Data Protection Laws.

4.2 Right to Audit. Customer shall have a right to audit Zoho's data processing facilities, practices and procedures against Applicable Data Protection Laws and this DPA, provided that:

(i) Customer shall, in the first instance, always try to obtain the required information by requesting from Zoho information specified under section 4.1;

(ii) where information provided by Zoho is not sufficient to demonstrate compliance with Applicable Data Protection Laws and this DPA, Customer:

(a) shall objectively demonstrate the insufficiency by enumerating the specific obligations under Applicable Data Protection Laws and/or this DPA that are not addressed by the information provided by Zoho under section 4.1 ("Possible Compliance Gap"); and

(b) may audit Zoho's data processing facilities, practices and procedures according to the audit procedure in section 4.3; and

(iii) Customer shall reimburse Zoho for any time expended for the audit at Zoho’s then-current professional services rates, which shall be made available to Customer upon request.

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

4.3 **Audit Procedure.** The procedure for audit is agreed as follows:

(i) A reasonably specific and detailed audit plan for the Possible Compliance Gap, the proposed audit date and the duration of the audit shall be communicated to Zoho according to the notice procedure at least 30 days prior to the proposed audit date.

(ii) Zoho shall review the proposed audit plan and provide Customer with any concerns or questions along with an estimate of the charges as specified under clause (iii) of section 4.2 based on the proposed duration of audit. Zoho shall cooperate with Customer to agree on a final audit plan.

(iii) The audit shall be performed only by individuals that have an appropriate level of expertise and qualification in the subject matter to perform the audit.

(iv) The audit shall be conducted during regular business hours at the applicable data processing facility, subject to the agreed final audit plan and Zoho's privacy, security and safety or other relevant policies and without unreasonably interfering with Zoho's business activities or compromising the security of Zoho's own data or other customers' data.

(v) Customer shall require the auditor to share the draft audit report to Zoho for review and incorporate reasonable changes suggested by Zoho.

(vi) Upon completion of the audit, Customer will promptly provide Zoho with a copy of the audit report.

4.4 **Confidentiality of Information Exchanged.**

(i) Customer acknowledges that all documents and information disclosed by Zoho under section 4.1, 4.2 and 4.3 and all interactions between the parties to the extent such interactions contain information about Zoho's systems and practices, including information observed or learnt by the auditor during audit and the draft and final reports ("Audit Information"), constitute Zoho's confidential information. Customer understands that unauthorized access, use or disclosure of Audit Information may cause irreparable injury to Zoho. Accordingly, Customer agrees to take, and to require the auditor engaged by Customer to take, reasonable measures to protect the confidentiality of the Audit Information from unauthorized access, use or disclosure.

(ii) Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements or confirming compliance with the requirements of this Data Processing Agreement by Zoho.

4.5 **Consequences of Material Non-Compliance.** In the event the audit reveals a material non-compliance by Zoho, Customer will not be required to pay the charges specified under clause (iii) of section 4.2 and Zoho shall reimburse the cost incurred by Customer for engaging the auditor for the audit

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

5. Sub-Processors

5.1 The parties agree that Zoho may engage Sub-Processors in the course of providing the services and with respect to Zoho's engagement of such Sub-Processors, the Customer hereby agrees that Zoho may authorise its affiliates and other third party entities as "Sub-Processors" in order to Process the Personal Data. In each case, any such Sub-Processor shall be permitted to Process Personal Data solely in accordance with Zoho's instructions and not for any other purpose. Zoho shall ensure that the Processing activity is carried out by the Sub-Processor in accordance with at least the same level of protection for the Personal Data and the rights of Data Subject as applicable to Zoho under Applicable Data Protection Laws. Zoho shall (i) make available to Customer the list of current Sub-Processors through the Privacy Policy statement applicable for the services; and (ii) provide email notification prior to appointment of any new Sub-Processor. Upon notification regarding Zoho's intention to engage a new Sub-Processor, Customer may object to such engagement by notifying Zoho promptly in writing within ten (10) business days after receipt of Zoho's notice. In the event Customer objects to a new Sub-Processor, as allowed in the preceding sentence, Zoho will recommend to the Customer commercially reasonable changes in the configuration or use of the services to avoid Processing of Personal Data by the proposed new Sub-Processor. If Customer is not satisfied with the changes suggested by Zoho, Customer may, upon written notice to Zoho, terminate the Service Agreement. In the event of such termination, Zoho will refund Customer on a pro-rata basis any amounts paid by Customer for use of the service.

5.2 Following written request from the Customer, Zoho agrees to promptly share copies of agreements executed with Sub-Processors. The parties agree that such agreements may be redacted to remove any commercial information or other clause unrelated to the Processing of Personal Data by Zoho.

6. Third Parties

6.1 In addition to Sub-Processors, Zoho has Customer's general authorisation for the engagement of third party service providers from the agreed list published by Zoho on its websites for providing: (a) specific functionalities of Zoho services; and (b) certain essential functions such as fraud detection, spam filtering and improvement of services ("Third Parties").

6.2 Customer may request Zoho for relevant information on processing by such Third Parties. Zoho shall, upon such request, make the information available to Customer.

6.3 Changes to the agreed list (whether addition or replacement of a Third Party), which apply to Customer's then current processing of personal data, will be communicated to Customer by email. Upon notification regarding such change by Zoho, Customer shall notify Zoho of its objection (if any) to processing by a Third Party, in writing, within 10 business days from the date of Zoho's notice. Customer may also object in writing to processing by a Third Party at any time during the term of Service Agreement.

6.4 If Customer objects to processing by a Third Party (as permitted by section 6.3), Zoho will recommend to Customer commercially reasonable changes in the configuration or use of the

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

services to avoid processing of personal data by the Third Party. If Customer is not satisfied with the changes suggested by Zoho, Customer may, upon written notice to Zoho, terminate the Service Agreement. In the event of such termination, Zoho will refund Customer on a pro-rata basis any amounts paid by Customer for use of the service

7. Other Obligations of Zoho

7.1. **Security of Personal Data.** Zoho agrees to implement appropriate technical and organisational security measures as specified under **Appendix 2** prior to and during Processing of any Personal Data to protect the security, confidentiality and integrity of the Personal Data and to protect the Personal Data against any form of accidental, unlawful or unauthorized Processing.

7.2. **International Transfers of Personal Data**. Zoho or any Sub-processor shall not process or transfer any Personal Data outside of the European Economic Area or the United Kingdom unless the transfer is compliant with Applicable Data Protection Laws.

7.3. **Confidentiality Obligations of Zoho Personnel.** Zoho shall ensure that its personnel engaged in the Processing of Personal Data and (i) are informed of the confidential nature of the Personal Data; (ii) are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

7.4. **Data Protection Impact Assessment.** Upon Customer's request, to the extent Customer does not otherwise have access to the relevant information and to the extent such information is available to Zoho, Zoho shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Applicable Data Protection Laws to carry out a data protection impact assessment with respect to Customer's use of the services.

7.5. **Data Subject Request and Assistance to Customer.** With respect to a request from a Data Subject to exercise the Data Subject's right to restrict Processing, right to erasure, right to rectification, right to access, right not to be subject to an automated individual decision making or data portability, the parties understand and agree upon the following:
(a) Zoho agrees to promptly notify the Customer about any request received directly from the data subjects without responding to that request. However, Customer agrees that Zoho is authorised to respond to the requests from data subjects before notifying Customer in order to establish that the request is in respect of Personal Data processed by Zoho on behalf of the Customer.

(b) Zoho shall assist Customer by implementing appropriate technical and organizational measures to enable the Customer to fulfil its obligation to respond to a Data Subject's request, to the extent that such assistance is to be provided under Applicable Data Protection Laws. Where Customer requests Zoho's assistance and Zoho has already enabled Customer to comply with such requests by implementing appropriate technical and organizational measures, Zoho shall have the right to charge the Customer for any reasonable costs or expenses incurred by Zoho in order to assist Customer with request(s) from Data Subjects.

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

7.6. **Data Incident Management and Notification.** Zoho has in place appropriate Security Incident management policies and procedures. In the event that Zoho becomes aware of a Security Incident involving data stored or otherwise Processed by Zoho or its Sub-Processors, Zoho will notify Customer without undue delay after becoming aware of the said Security Incident. Zoho will take all commercially reasonable efforts to remediate the Security Incident and prevent recurrence. Customer acknowledges that Zoho's obligation specified herein shall not apply to Security Incidents caused by Customer or its authorized users.

7.7. **Return or deletion.** Upon termination or expiration of the Service Agreement, the parties acknowledge and agree that (i) Return of personal data processed by Zoho should be achieved via Customer initiating the export of such personal data via the user interface made available by Zoho;(ii)Zoho will automatically delete personal data processed by Zoho at the next routine clean-up cycle from the primary servers (that occurs once in 6 months). The data deleted from primary servers will be deleted from backups 3 months thereafter; and (iii) Zoho will provide confirmation of the completion of the relevant clean-up cycle as certification of deletion of the personal data. Such certificate will be provided only upon request from Customer.

7.8. **Data Protection Officer**. Zoho has appointed a data protection officer who may be reached at dpo@zohocorp.com.

8. Order of Precedence

In the event of a conflict between the provisions of this DPA and those of the Service Agreement in respect of the Processing and protection of Personal Data, the provisions of this DPA will prevail. Except as expressly modified herein, all terms and conditions of the Service Agreement shall remain in full force and effect.

9. Governing law and Jurisdiction

This DPA shall be governed by and construed strictly in accordance with the laws of England and Wales. Any dispute arising out of or resulting from this DPA shall be subject to the exclusive jurisdiction of courts in England and Wales to the exclusion of all other courts.

This DPA has been entered into on the date stated at the beginning of it.

Executed for and behalf of **Customer** by:	Executed for and behalf of **Zoho** by:
Shelley James ..... (signature)	S. Iyengar .....(signature)
Shelley James ..... (print name)	Sridhar Iyengar .....(print name)
Co-founder ..... (position)	Director .....(position)

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

Appendix 1

Customer

The Customer has subscribed to Zoho's online collaboration and management tools as part of its business.

Zoho

Zoho is a provider of services for online collaboration and management, including word processor, spreadsheet, presentation tool, database application creator, email client, chat client, organizer, customer relationship management application and project management application services.

Data subjects

The Personal Data Processed concern the following categories of Data Subjects:

Zoho may Process any data inputted by authorised users of Zoho's online collaboration and management tools. Primarily, this will relate to living individuals who are:

- users who are authorised by Customer to use the services
- employees, agents, contractors, and contacts of the Customer
- prospects, customers and clients, business partners and vendors of the Customer
- advisers and professional experts of the Customer
- employees, agents, contractors, and contacts of the Customer's prospects, customers and clients, business partners, vendor, advisers and professional experts

Categories of data

The Personal Data Processed concern the following categories of data:

Zoho may Process any data inputted by authorised users of Zoho's online collaboration and management tools. Primarily, this will relate to the following categories of data:

Name, contact details, address

Employment related data

Financial information

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

Special categories of data (if appropriate)

The Personal Data Processed concern the following special categories of data:

As the services allow for free text input, there may be occasions when the following details are inputted in relation to a Data Subject:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- information about physical or mental health
- sexual life
- the commission or alleged commission by the Data Subject of any offence
- any proceedings for any offence committed or alleged to have been committed by the Data Subject, the disposal of such proceedings or the sentence of any court in such proceedings

Processing operations

The Personal Data Processed will be subject to the following basic Processing activities:

The Processing activity of Zoho will include the performance of the services pursuant to the terms of the Customer's Service Agreement with Zoho.

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

Appendix 2

Description of the technical and organisational security measures to ensure the security of the data:

Technical and Organizational Security Measures applicable to the Cloud services offered by Zoho

Zoho has established, and will maintain at a minimum, an information security management system that includes the following:

Security Governance

1. A governance framework that supports relevant aspects of information security through appropriate policies and standards.
2. Formal documentation of the roles and responsibilities of employees with respect to governance of Information Security within Zoho that are communicated by the management to employees.
3. An information security program in accordance with the international standard ISO 27001 that includes technical, organizational and physical security measures in order to protect personal data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction.
4. Formally documented information security policy, data privacy policy and other policies that are communicated periodically to employees responsible for the design, implementation and maintenance of security and privacy controls. The policies will be reviewed annually to keep them up-to-date.
5. Compliance with industry standard security measures as described at https://www.zoho.com/compliance.html.

Risk Management

1. Annual risk assessment, to prioritize mitigation of identified risks.
2. Established internal audit requirements and periodical audits on information systems and processes at planned intervals.
3. Assessment of the design and operating effectiveness of controls against the established control framework through which corrective actions related to identified deficiencies will be tracked to resolution.

Human Resources Security

1. Background verification of all employees having access to confidential data that includes verification of criminal records, previous employment records if any, and educational background.

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

2. Signing of confidentiality agreement and acceptable use policy by employees upon their employment with clauses on protection of confidential information.
3. Training on security and privacy awareness including training on Zoho's policies, standards and relevant technologies along with maintenance and retention of training completion records.
4. Employees will be required to adhere to the information security policies and procedures. Disciplinary process for non adherence will be defined and communicated.

Identity and Access management of Zoho Personnel

1. Creation of unique identifiers for employees to access information systems and prohibition of sharing user accounts among employees.
2. User authentication to information systems protected by passwords that meet Zoho's password policy requirements derived based on NIST SP 800-63B standards.
3. Strong password configurations that include i) 8 character minimum length; ii) non dictionary words and iii) screening of passwords against list of known compromised passwords.
4. Mandatory Two factor authentication for access to information systems involving confidential data.
5. Secure remote access to the corporate network provisioned via SSL VPN with strong encryption and two factor authentication.
6. Adherence to the principles of least privilege and need-to-know and need-to-use basis for access control.
7. Approval mechanism from appropriate personnel to provide access to information systems.
8. Revocation of access that is no longer required in the event of termination or role change.
9. Recording of approval, assignment, alteration and withdrawal of access rights.
10. User access reviews on a half yearly basis and corrective actions whenever necessary.
11. Restrictions on administrative access to personal data and provision of access on a strictly need-to-know basis along with implementation of access-control measures such as mandatory two factor authentication.

Asset Management

1. Inventory maintenance of assets associated with information processing. Owners are assigned for each asset and rules for acceptable use of assets are defined. Assets assigned to employees are returned in the event of termination or role change.
2. Capacity management policies through which resources are continuously monitored and projections are made for future requirements.
3. Determined procedures in accordance with industry best practices for the reuse, secure disposal and destruction of electronic media to ensure that the data is rendered unreadable and unrecoverable.

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

4. Disposal of unusable devices by verified and authorized vendors which includes storing of such devices in a secure location until disposal, formatting any information contained in the devices before disposal, degaussing and physical destruction of failed hard drives using shredder and crypto-erasing and shredding of failed SSDs.

Physical Security

1. Physical access to Zoho's data center is highly restricted and requires prior management approval. The data centers are housed in facilities that require electronic card key access. Additional two-factor authentication and biometric authentication are required to enter the data center premises and there is continuous monitoring of CCTV cameras and alarm systems.
2. Control of physical access to Zoho's development facilities using access cards and monitoring by security personnel.
3. Installation of CCTV cameras and review of access logs and CCTV footage in case of any incidents.
4. Defined visitor management process to authorize visitor entries and maintenance of access records of visitors.
5. Revocation of physical access to employees in the event of termination of employment or role change.

Network Security and Operations

1. A dedicated Network Operations Center (NOC), which operates 24x7 monitoring the infrastructure health.
2. Establishment and implementation of firewall rules in accordance to identified security requirements and business justifications.
3. Review of firewall rules on a quarterly basis to ensure that legacy rules are removed and active rules are configured correctly.
4. Establishment and maintenance of appropriate network segmentation, that includes use of virtual local area networks (VLANS) where appropriate, to restrict access to systems storing confidential data with a data storage layer that is designed to be not directly accessible from the Internet.
5. Clear separation of production, development and integration environments to ensure that production data is not replicated or used in non-production environments for testing purposes.
6. Management of access to production environments by a central directory and authentication for such access using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Access to the production environment is facilitated through a separate network with strict rules.
7. Deployment of DDOS mitigation capabilities from well established service providers to

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

prevent volumetric attacks and to keep the applications available and performing.

Secure Software Development

1. Well defined security process that is implemented and monitored throughout the SDLC taking into consideration confidentiality, availability and integrity requirements.
2. Implementation of secure software development policies, procedures, and standards that are aligned to industry standard practices such as OWASP, CSA, CWE/SANS including secure design review, secure coding practices, risk based testing and remediation requirements.
3. Training on secure coding principles and industry standards to personnel involved in the development and coding of products.
4. "Secure by design" approach by incorporating security risk assessments and Threat modeling in the planning and analysis phase of SDLC and review of the design to prevent new threats.
5. Examination of Source code changes for potential security issues using Zoho's proprietary SAST (static code analysis) tools and manual review process before deployment.
6. Web Application Firewall (WAF) layer that is embedded in all web applications for protection against Open Web Application Security Project (OWASP) threats, including SQL injections, Cross-site scripting (XSS) and remote file inclusions.
7. Maintenance of inventory of third party software that gets bundled in the products/services.
8. Alerts on potential security vulnerabilities in the third party software by Zoho's proprietory SCA (Software Composition Analysis) that is reviewed periodically to check its applicability and impact and to take steps to upgrade third party software to the latest version.
9. Appropriate checking and elimination procedures to ensure that the service is not affected by malware/viruses during development, maintenance and operation.
10. Appropriate security controls to ensure the confidentiality, integrity and availability of the CI/CD pipeline in the software development environment used to develop, deploy, and support the products.
11. Maintenance of clear distinction between the development, QA and production environments.

Data Security and Management

1. Information classification scheme with data handling guidelines related to access control, physical and electronic storage, and electronic transfer.
2. Logical separation of each customer's service data from other customers' data by distributing and maintaining separate logical cloud space for each customer.
3. Deletion of data from active database upon termination of Zoho services by the customers (clean-up occurs once in every 6 months), deletion of backup data within 3 months of deletion from active database and termination of accounts that remain unpaid and inactive

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

for a continuous period of 120 days by giving prior notice to the customer.

Cryptography

1. Use of transport encryption for information that traverses across networks outside of the direct control of Zoho including, but not limited to the Internet, Wi-Fi and mobile phone networks.
2. Encryption of data transmission to Zoho services are made using TLS 1.2/TLS1.3 protocols, with latest and strong ciphers like AES_CBC/AES_GCM 256 bit/128 bit keys, authentication of message using SHA2 and use of ECDHE_RSA as the key exchange mechanism.
3. Encryption of sensitive data at rest using 256-bit Advanced Encryption Standard (AES). (The data that is encrypted at rest varies specific to Zoho services and also options are provided where the customer defines the fields to encrypt depending on their business need and data sensitivity).
4. Irreversible industry standard algorithm (bcrypt) will be used to hash and store the passwords of Zoho services with randomly generated per user salt added to the input.
5. Zoho's in-house Key Management Service (KMS) to own and maintain encryption keys that includes additional layer of security by encrypting the data encryption keys using master keys.
6. Separation of master keys and data encryption keys by physically storing them in different servers with limited access.

Change Management

1. A change management policy that governs changes in all components of the service environment whereby all changes are planned, tested, reviewed and authorized before implementation into production.
2. Assessment of the potential impacts, including information security and privacy impacts of the changes.
3. Documented fall-back mechanisms including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
4. Notification to customers of any changes that may affect customers in an adverse manner.

Configuration Management

1. Implementation of security hardening and baseline configuration standards in accordance with industry standards that are reviewed and updated periodically.
2. Predefined OS images with security baselines are used to build systems in development and production.
3. Hardening standards including (i) ensuring that unnecessary features, services, components, files, protocols and ports are removed from the production environment; and (ii) removing

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

unnecessary user logins and disabling or changing default passwords.

4. Approval from the appropriate personnel to install any software package in the production environment.

Vulnerability Management

1. Vulnerability management plan designed to (i) identify promptly, prevent, investigate, and mitigate any cyber security vulnerabilities; (ii) analyze the vulnerability; (iii) perform recovery actions to remedy the impact.
2. Vulnerability assessments using automated scanners performed periodically on Zoho's internet facing systems.
3. Application penetration testing by Zoho's in house security personnel performed annually in accordance to defined test methodologies.
4. Review of identified issues from vulnerability assessments and penetration testing, determination of its applicability, impact and priority and rectification in accordance with the SLA definition: High level vulnerabilities within 7 calendar days of discovery, Medium level vulnerabilities within 30 calendar days of discovery and Low level vulnerabilities within 60 calendar days of discovery.
5. Monitoring known vulnerabilities from common sources such as OWASP, CVE, NVD and other vendor security lists and installation of security relevant patches to product and/or supporting systems in accordance with Zoho's patch management policy.
6. Antivirus deployment by running the current version of industry standard anti-virus software as a part of which signature definitions are updated periodically within 24 hours of release, real time scans are enabled and alerts are reviewed and resolved by appropriate personnel.

Security Logging and Monitoring

1. Use of centralized logging solution to aggregate and correlate events from various components including network devices, servers and applications.
2. Maintenance of audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events and retention of logs in accordance with applicable policies and regulations.
3. Host and application intrusion detection (IDS) technology to facilitate timely detection, investigation and response to incidents.
4. Restrictions on physical and logical access of logs by authorized personnel.

Business continuity and Disaster recovery

1. Disaster recovery and business continuity plans and processes (i) to ensure continuous availability of the services in case of any disaster; (ii) to provide an effective and accurate recovery.
2. Annual review of business continuity plan to evaluate its adequacy & effectiveness.

Zoho Sign Document ID: 4AC8C6031-_DHXA0YWLQP99UF2LSTJHUUEDWIFQSRLF5QBX65TZMM

3. Redundancy mechanisms to eliminate single point of failure consisting of (i) dual or multiple circuits, switches, networks or other necessary devices; and (ii) storing of application data in a resilient storage that is replicated in near real time across data centers.
4. Taking periodic backups (incremental backups every day and weekly full backups) and storing them in an encrypted format both in primary and secondary datacenter.
5. Retention of backups for a period of three months and testing recovery of backups at planned intervals.
6. SLA for service availability with 99.9% monthly uptime as a part of which real time availability can be viewed in https://status.zoho.com.

Incident Management

1. An incident response plan and program containing procedures that are to be followed in the event of an information security incident.
2. Dedicated email (incidents@zohocorp.com) to which external parties can report security incidents and creating awareness among employees to report any potential security incident or weakness on time without any delay.
3. Tracking of security incidents, fixing of such incidents through appropriate actions, maintenance of such records in the incident registry and implementation of controls to prevent recurrence of similar incidents.
4. Incident management procedures that lays down the steps for notifying the client, and other stakeholders in a timely manner in accordance with breach notification obligations.
5. Implementation of appropriate forensic procedures including chain of custody for collection, retention, and presentation of evidence in the event of an information security incident likely to result in a legal action.

Third-Party Vendor Management

1. Vendor management policy through which Zoho evaluates and qualifies third party vendors as a part of which new vendors are onboarded only after understanding their processes and performing risk assessments.
2. Execution of agreements with vendors that require vendors to adhere to confidentiality, availability, and integrity commitments in order to maintain Zoho's security stance.
3. Annual reviews to monitor the operation of vendor's processes and security measures.