DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is made effective as of _____ between the parties listed in Annex I of Schedule 1 (each a "**Party**").

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

(B) The Parties acknowledge that, during the provision of services, personal data will be processed by Zoho. Accordingly, the Parties enter into this DPA for the purposes and scope mentioned under Clause 1 of the Schedule 1.

(C) This DPA includes the Schedule(s) and Annexures. Any reference to this DPA includes reference to the Schedule(s) and Annexures.

PARTIES HEREBY AGREE AS FOLLOWS:

1. **Instructions:** For the purposes of Clause 7.1 of the Schedule 1, Customer agrees that its instructions to Zoho for processing personal data are:

    a. to process such data strictly in accordance with the Service Agreement and this DPA;

    b. to process data where such processing is initiated by Customer via the user interface of the Zoho services;

    c. to process data for fraud prevention, spam filtering, and service improvement, including automation; and

    d. 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.

2. **Documentation and Compliance:** For the purposes of Clause 7.6 of the Schedule 1:

2.1 Demonstration of Compliance. Upon request by Customer, Zoho will demonstrate its compliance with GDPR 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 GDPR, or approved code(s) of conduct as specified under the GDPR.

2.2 Right to Audit. Customer shall have a right to audit Zoho's data processing facilities, practices and procedures against GDPR 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 2.1;

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

(a) shall objectively demonstrate the insufficiency by enumerating the specific obligations under GDPR and/or this DPA that are not addressed by the information provided by Zoho under section 2.1 ("Possible Compliance Gap"); and

(b) may audit Zoho's data processing facilities, practices and procedures according to the audit procedure in section 2.3; 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.

2.3 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 2.2 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.

2.4 Confidentiality of Information Exchanged.

(i) Customer acknowledges that all documents and information disclosed by Zoho under section 2.1, 2.2 and 2.3 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.

2.5 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 2.2 and Zoho shall reimburse the cost incurred by Customer for engaging the auditor for the audit.

2.6 Role of Parties

Where the Customer acts as the Controller of the personal data, Zoho will be a processor of such data; where the Customer is by itself a Processor of the personal data acting on behalf of it's group entities, Zoho will be a sub-processor of such personal data.

The Parties agree that the Customer will be Zoho's sole point of contact and Zoho shall process the personal data solely as per Customer's Instructions as described in section 1

Customer shall ensure that its instructions to Zoho are in consonance with the instructions of the Controller.

3. Use of Sub-processors

For the purposes of Clause 7.7 of the Schedule 1:

a. The agreed list of sub-processor is published by Zoho on its websites. Customer may request Zoho for relevant information on processing by such sub-processors. Zoho shall, upon such request, make the information available to Customer.

b. Changes to the agreed sub-processor list (whether addition or replacement of a sub-processor), which apply to Customer's then current use of the service, 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 sub-processor engaged by Zoho, in writing, within 10 business days from the date of Zoho's notice. Customer may also object in writing to processing by a sub-processor at any time during the term of Service Agreement.

c. If Customer objects to processing by a sub-processor (as permitted by Clause 7.7 of the Schedule 1 and section 3b), Zoho will recommend to Customer commercially reasonable changes in the configuration or use of the services to avoid processing of personal data by the 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.

4. Third Parties

4.1 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"**).

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

4.3 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.

4.4 If Customer objects to processing by a Third Party (as permitted by section 4.3), Zoho will recommend to Customer commercially reasonable changes in the configuration or use of the 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.

5. International Transfers

5.1 For the purposes of Clause 7.8, Customer understands that personal data; (i) will be stored in Zoho's data centers in the European Economic Area (EEA); (ii) may be accessed on a need basis by applicable Zoho group entities as described in Schedule 2; and (iii) will be transferred outside EEA to the sub-processors and Third Parties depending on the Zoho services used by Customer. Customer agrees that such transfers of personal data are necessary for providing the services and will be deemed as instructions by Customer.

5.2 Where Zoho transfers personal data to Zoho group entities, sub-processors, or Third Parties located outside EEA, Zoho shall ensure that a valid basis of transfer as required by GDPR is in place.

6. Data Subject Requests

6.1 For the purposes of Clause 8(a), Customer authorizes Zoho to respond to the requests from data subjects before notifying Customer, to determine if the request is with respect to the personal data processed by Zoho on behalf of the Customer.

6.2 For the purposes of Clause 8(b), Zoho shall implement technical and organizational measures to enable Customer to comply with requests from data subjects who wish to exercise their rights such as 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. Where Customer requests Zoho's assistance (under this section and Clause 8) 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.

7. Other Assistance to the Controller

7.1 For the purposes of Clause 8(c), Parties agree that Zoho's obligation to assist Customer in its obligation to (i) conduct a data protection impact assessment; and (ii) consult the competent supervisory authority/ies, is limited to providing the relevant information to Customer.

7.2 For the purposes of Clause 9.1, Parties agree that Zoho's obligation to assist the Customer in notifying the supervisory authority and in notifying the data subjects is limited to: (i) the extent such breach involves personal data processed by Zoho on behalf of the Customer; and (ii) providing relevant information about the breach to Customer, if such information is available to Zoho and otherwise not available to Customer.

8. Return and Deletion of Data

For the Purposes of Clause 10(d), Customer acknowledges and agrees that:

a. 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;

b. 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

c. 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.

9. Governing Law and Jurisdiction

9.1 This DPA shall be governed by and construed strictly in accordance with the laws of the Netherlands (excluding the rules governing conflict of laws).

9.2 Any dispute arising out of or resulting from this Agreement shall be subject to the exclusive jurisdiction of courts in Amsterdam to the exclusion of all other courts.

10. DPA to Supersede Prior Agreements

Parties agree that this DPA will supersede and prevail over all the previous data protection and privacy agreement(s) between Customer and Zoho.

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1 (Purpose and scope)

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of 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/"GDPR").

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of GDPR.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of GDPR.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of GDPR.

Clause 2 (Invariability of the Clauses)

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(**b)** This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 (Interpretation)

(a) Where these Clauses use the terms defined in GDPR, those terms shall have the same meaning as in the GDPR.

(b) These Clauses shall be read and interpreted in the light of the provisions of GDPR.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 (Hierarchy)

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 (Docking clause)

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6 (Description of processing(s))

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 (Obligations of the Parties)

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be

given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the GDPR or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from GDPR. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to GDPR.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of GDPR.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of GDPR, the processor and the sub-processor can ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of GDPR, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 (Assistance to the controller)

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) The obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) The obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) The obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) The obligation in Article 32 of GDPR.

(5) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 (Notification of personal data breach)

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of GDPR, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) In notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) In obtaining the following information which, pursuant to Article 33(3) of GDPR, shall be stated in the controller's notification, and must at least include:

(1) The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) The likely consequences of the personal data breach;

(3) The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) In complying, pursuant to Article 34 of GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of GDPR.

SECTION III

FINAL PROVISIONS

Clause 10 (Non-compliance with the Clauses and termination)

(a) Without prejudice to any provisions of GDPR, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The

processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) The processor is in substantial or persistent breach of these Clauses or its obligations under GDPR.

(3) The processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to GDPR.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]* **("Customer")**

Name: _____

Address:_____

_____

Signature _____

Name _____

Title _____

Date _____

Contact _____

Processor(s):

Name: Zoho Corporation B.V **("Zoho")**

Address: Beneluxlaan 4B, 3527 HT UTRECHT, The Netherlands

Signature _____

Name _____

Title _____

Date _____

Contact privacy@eu.zohocorp.com

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed:

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 personal data processed:

Categories of personal data processed may include, but are not limited to:

Name, contact details, address

Employment related data

Financial information

Sensitive data processed (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:

Zoho provides options to encrypt sensitive data at rest. The ability to encrypt data at rest is different in each Zoho service and it may not be enabled by default. The details of encryption capabilities in Zoho services are either published by Zoho on its websites or available to Customer upon request. Based on the nature of the sensitive personal data processed, Customer shall determine

the suitability or adequacy of encryption capabilities provided by Zoho service(s) and enable encryption.

Nature of the processing: The nature of processing by Zoho will include the provision of Zoho services pursuant to the terms of Service Agreement, this DPA or any other agreement between Customer and Zoho.

Purpose(s) for which the personal data is processed on behalf of the controller: To provide Zoho services in accordance with instructions provided by Customer as described under section 1 of this DPA.

Duration of the processing: Duration of the Service Agreement

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing:
As specified under section 3, Sub-processor(s) will process personal data for the duration of the Service Agreement.

Annex - III

Technical and Organizational Security Measures applicable to Manage Engine Service Desk

Plus

Introduction

ManageEngine makes IT management solutions that enable IT admins address their IT challenges proactively. We improve our customers' security posture and prioritize their data security and privacy. In this article, we document our security processes at the organizational and product levels.

I. Organization security

We have an Information Security Management System (ISMS) in place which takes in into account our security objectives as well as the risks and mitigation concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

Employee background checks

Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

Security Awareness

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles. We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

Dedicated security and privacy teams

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They regulate and maintain defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

Internal audit and compliance

We have a dedicated compliance team to review procedures and policies in ManageEngine to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards.

This team also does periodic internal audits and facilitates independent audits and assessments by third parties. For more details, check out our compliance portfolio.

Endpoint security

All workstations issued to ManageEngine employees run up-to-date OS versions and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by ManageEngine's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

II. Application security

ServiceDesk Plus is a help desk management platform that includes core help desk and IT management applications and project management, contract management, asset management, CMDB, and features for ITIL (information technology infrastructure library) compliance. ServiceDesk Plus is currently used by various organizations; some of them have installed and configured ServiceDesk Plus within their network whereas few others have installed and configured ServiceDesk Plus to be accessed over the internet. So, any compromise on the security of customer data will expose organizations to serious risks. Therefore, ServiceDesk Plus is designed to offer maximum security at all times, including application installation, user authentication, data transmission, storage, and regular use.

Secure by design

Our Software Development Life Cycle (SDLC) model mandates our ServiceDesk Plus engineering team to strictly adhere to our secure coding standards. In addition, we adhere to security standards across the SDLC process.

Security standard during the analysis and design phase.

- Our engineering team gathers and analysis requirements to identify any security flaws and loopholes in new features.
- Prepares a vulnerability assessment plan to address security concerns posed by users and security analysts in the previous releases/versions.
- Develops a product or feature prototype, including changes and subjects them to the change management authority for approval.

Security standard during the development phase

- The development team follows the security guidelines given by the product security team.
- The source code is periodically reviewed by the security coordinator and team lead.
- Before using any third-party code dependencies and libraries, our legal and security teams will verify whether the third party libraries have any known security issues or not.
- Only authorized engineers can access the source code repository.

- Approval/review process is enabled for modified sources.

Security standard during the QA/release phase

- Performs integration, automation, and penetration tests to ensure that the new features or modules are secure from potential vulnerabilities/flaws.
- Continuous smoke testing to ensure that the core functionality of the product remains intact without opening new security loopholes.
- Generates security assessment reports to identify further areas of improvement.
- Runs continuous vulnerability scans post release for timely identification and patching of vulnerabilities.

Security review process

We have a security team to ensure the released build/product is free from security vulnerabilities. The team will follow the below process during the security review process.

- Runs automated security audit tool on new features.
- Conducts a security audit program for all features and bug fixes.
- Analyze third-party files usage and its known vulnerabilities.
- Collects brief feature/bug fixes details from developers to discover possible vulnerabilities.
- Creates security briefs for both developers and support team to provide instant solution to customers.
- Monitors recently discovered vulnerabilities.
- As a final check, white box testing, i.e. manual source code review, is also carried out by the security team to discover any defects in the build. In this stage, the security team develops test cases to verify the proper working of all functionalities and error handling of the developed feature.
- Once all issues are resolved and a fresh build is created, the security team will approve the build as final.

Other security standards

- Our repository and build infrastructure are secured with SSH/HTTPS protocol and are placed in a secure, segmented network with stricter authentication and access controls.
- Our security and code frameworks are OWASP-compliant and implemented at the application layer.
- All code changes, third-party dependencies, release bundles, and upgrade packs are subject to multiple levels of internal security review, automation, and penetration testing efforts, and vulnerability scans to ensure they are well secured from logical bugs and security issues.
- Every update and new feature in ServiceDesk Plus is subject to internal change management policies and regular vulnerability assessments, and changes are implemented into production only if approved by the concerned change and security management authorities.
- The binaries are signed with a code signing certificate and the private key is securely stored in the segmented network with limited access.

- The ServiceDesk Plus engineering team works closely with internal security teams to obtain their feedback and identify areas of improvement to strengthen our security posture.

Besides the security measures described above, we are continuously striving to make the application more secure. The following section provides comprehensive details about security specifications of ManageEngine ServiceDesk Plus.

ServiceDesk Plus: Security specifications

Refer to the below link to know more about product security specifications.

https://www.manageengine.com/products/service-desk/servicedesk-plus-security-specifications.html

III. Operational security

Customer data protection in ServiceDesk Plus

ServiceDesk Plus is an installable product, so all data resides in the customer environment. Therefore, data breach is not possible in the ServiceDesk Plus On Premises version. Only customer's support tickets and log files are stored in our customer support portal.

- The files uploaded by customers are stored securely in a customer support portal.
- The uploaded files are accessible only to authorized support technicians.
- Data uploaded in server will be kept confidential and will be used for debugging purposes only.
- The uploaded files are allowed to download only in specific servers and the server credentials are not shared to anyone.
- The uploaded files will be removed automatically in the following conditions.
    - During ticket closure, we ensure the log & data files are deleted in the server.
    - File uploaded in server will be deleted automatically after 25 days.

Build and patching process

- The ServiceDesk Plus team works closely with the MESRC to run mandatory vulnerability scans and penetration tests before every major release to ensure that latest builds are completely foolproof. In addition, the team runs continuous vulnerability assessments on these builds to ensure that they are free from any new vulnerabilities.
- Users are notified immediately to upgrade to the latest version as and when there is a new security patch or update.
- In the event of a security concern or escalation, users are requested to submit a detailed report on the vulnerability or security bug. Meanwhile, the product team evaluates the validity and risks associated with the bug and prioritizes the release based on its severity.

Logging and monitoring

Product logs certain data for debugging and to prevent any misuse.The log files generated by ServiceDesk Plus are stored in customer machines. A maximum of 50 log files can be stored with the size capped to 10 MB for each file. Once this limit is reached, the log files are rolled over; the older files are removed from user machines. We do not have access to the log files unless the user shares it to avail support services. In this case, only the support staff and development team, limited by their roles, have access to the log files. After the issue is identified, the log files are deleted.

Business Continuity

We have backup power, temperature control systems, and fire-suppression and fire-protection systems to ensure business continuity. Dedicated business continuity plans are present for major operations such as infrastructure management and technical support. We have a well planned business continuity and disaster recovery plan in place to assist us in the event of extended service outages, thereby affecting the services provided to the customers by factors beyond our control e.g., natural calamities, man-made disasters, etc., to resume endpoint management operations to the maximum possible extent within a minimal time frame. The plan encompasses all our internal operations to ensure continued services for our customers. We have three recovery teams namely, the Emergency Management Team (EMT), the Disaster Recovery Team (DRT), and the IT Technical Services (IT) team, in place for better coordination and support among various teams.

IV. Incident Management

Reporting

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will provide you with necessary evidence regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations. We respond to the security or privacy incidents you report to us through incidents@zohocorp.com, with high priority. For general incidents, we will notify users through our blogs, forums, and social media. For incidents specific to an individual user or an organization, we will notify the concerned party through email (using their primary email address of the Organization administrator registered with us).

Breach Notification

As data controllers, we notify the concerned Data Protection Authority of a breach within 72 hours after we become aware of it, according to the General Data Protection Regulation (GDPR). Depending on specific requirements, we notify the customers, when necessary.

V. Responsible Disclosure

We have a vulnerability reporting program called "Bug Bounty", which recognizes and rewards the work of security researchers in identifying vulnerabilities. We are committed to working with the community to verify, reproduce, respond, legitimate, and implement appropriate solutions for the reported vulnerabilities. If you happen to find any, please submit the issues at https://bugbounty.zoho.com. If you want to report vulnerabilities to us directly, mail us at support@servicedeskplus.com

I. Organization security

We have an Information Security Management System (ISMS) in place which takes into account our security objectives as well as the risks and mitigation concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

Employee background checks

Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

Security Awareness

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles. We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

Dedicated security and privacy teams

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They regulate and maintain defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

Internal audit and compliance

We have a dedicated compliance team to review procedures and policies in ManageEngine to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards. This team also does periodic internal audits and facilitates independent audits and assessments by third parties.

For more details, check out our compliance portfolio.

Endpoint security

All workstations issued to ManageEngine employees run up-to-date OS versions and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by ManageEngine's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

II. Application security

i. Secure by Design

We adhere to the secure coding guidelines of the Software Development Life Cycle (SDLC) and these guidelines are shared with all developers. As the next step, we screen the code changes to look for potential security issues by first, manually reviewing it, and second, using our code analyzer, and vulnerability scanner tools. This entire process is carried out before the release of any new feature. If any issue is found, they are immediately checked and fixed. Furthermore, a robust security framework, that is based on the OWASP standards, is implemented in the application layer. This framework provides means to mitigate threats such as SQL Injection, Cross-Site Scripting, and Application Layer DoS attacks. To top it all, we conduct regular sessions to educate developers about secure coding practices.

ii. Identity and Access control

- **Role-Based Access Control**

Role-Based Access Control allows only authorized users to access a specific function. Users are designated with specific roles and their access to each functionality depends on the permission granted to them.

iii. Encryption

- **In transit:**

- Any data transfer from the agent application to the server happens using the strong encryption protocol, HTTPS. Users can set HTTPS as the default protocol for all communication from the web console.
- Users can disable older version of TLS in the server.xml. The support for older version of TLS is provided to enable users to manage their running on older Windows versions. Additionally, TLS 1.2 and strong ciphers are supported for the latest systems.

This ensures that the data is always encrypted during its transfer.

●**At rest:** Sensitive data, such as passwords, auth-tokens, and the like, that are stored in databases are encrypted using 256-bit Advanced Encryption Standard (AES).

Database Protection: The product database can be accessed only by providing instance-specific credentials and is limited to local host access. The passwords stored are one-way hashed using bcrypt and are filtered from all of our logs. As bcrypt hashing algorithm with per-user-salt is used, it would be exorbitant and heavily time-consuming to reverse engineer the passwords and the database resides in Customer setup only.

3.Operational security

a.**Customer data security:** The customer data resides only in their environment, as the product is an on-premise solution.

Note: In case any customer requires help in resolving any issue, we may require the customer's logs. The customer uploads the logs through a secure portal owned by us, that can be accessed only by authorized personnel and grants us permission to access them. The logs will be deleted automatically after five days from the time of upload. In addition to this, any breaches that occur will be notified to the customer.

b.Vulnerability and patch management:

We have a dedicated vulnerability process that actively scans for security threats or vulnerabilities using a combination of certified third-party scanning tools, and in-house tools. Subsequently, automated and manual testing is performed. Furthermore, the security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to identify security incidents that might affect the company. Once we identify a vulnerability that requires remediation, it is logged, prioritized according to severity, and is assigned an owner. We further identify the associated risks and mitigate them by either patching the vulnerable systems or applying relevant controls.

After assessing the severity of the vulnerability based on the impact analysis, we commit to resolve the issue within our defined SLA. Depending upon the severity, we send the security advisories to all our customers describing the vulnerability, the patch and the steps to be taken by the customer.

c.Business continuity:

●We have backup power, temperature control systems, and fire-suppression and fire-protection systems to ensure business continuity. Dedicated business continuity plans are present for major operations such as infrastructure management and technical support.

●We have a well planned business continuity and disaster recovery plan in place to assist us in the event of extended service outages, thereby affecting the services provided to the customers by factors beyond our control e.g., natural calamities, man-made disasters, etc., to resume endpoint management operations to the maximum possible extent within a minimal time frame. The plan encompasses all our internal operations that ensures continued services for our customers. We have three recovery teams namely, the Emergency Management Team (EMT), the Disaster Recovery Team (DRT), and the IT Technical Services (IT) team, in place for better coordination and support among various teams.

d.Responsible Disclosure

A vulnerability reporting program in "Bug Bounty", to reach the community of researchers is in place, which recognizes and rewards the work of security researchers. We are committed to working with the community to verify, reproduce, respond, legitimate, and implement appropriate solutions for the reported vulnerabilities.
If you happen to find any, please submit the issues at https://bugbounty.zoho.com or mail us at: opmanager-support@manageengine.com.

e.Customer controls for security

So far, we have discussed what we do to offer security on various fronts to our customers. Here are the things that you as a customer can do to ensure security from your end:

●Choose a unique and complex password.
●Secure Network shared folders.
●Use trusted third party certificates to ensure secured connections.
●Check for latest patches and update your endpoints regularly.
●https://www.manageengine.com/network-monitoring/service-packs.html