BEEKEEPER
DATA PROCESSING AGREEMENT

Between

Beekeeper AG
Hardturmstrasse 181
8005 Zürich
Switzerland

(Beekeeper AG as “Processor”)

and

(as “Controller”, if not defined otherwise on page 1)

This **Data Processing Agreement** (DPA) is for the parties to establish an agreement on the roles and responsibilities within the framework of the listed **Principles,** between the **Processor** (Beekeeper AG, Hönggerstrasse 65, 8037 Zurich, Switzerland) and the **Controller**:

Whereas the intention of the Processor is to:

1. Provide a DPA in compliance with Section 2 Art. 4, of the Swiss Federal Act on Data Protection (FADP:1992) and any applicable Swiss Cantonal directives or regulations on Data Protection and Privacy including any revisions then after;

2. In compliance to Section 2 Art. 7 of the Swiss Federal Act on Data Protection (FADP:1992) and any applicable Swiss Cantonal directives or regulations on Data Protection and Privacy including any revisions then after;

3. Process the personal and other data only further to documented instructions from the Controller, including restriction of access by other parties not a signatory to this DPA, or transfer of personal data to third countries or international organizations, unless provided otherwise by Swiss or agreed Cantonal law to which the Processor is subject;

4. Take all appropriate technical and organizational measures including breach management and notification;

5. Achieve transparency with the use of all sub-processors and third party companies towards the Controller,

6. Impose on its sub-processors the data protection obligations set out in the commercial agreement (or legal act) between the Controller and the Processor;

7. Taking into account the nature of the processing, assist the Controller by taking appropriate technical and organizational measures, insofar as possible, to ensure fulfilment of the Controller obligation to reply to requests by data subjects exercising their rights;

8. Assist the Controller in ensuring compliance with its security and certain other obligations, taking into account the nature of the processing and the information available to the Processor;

9. At the Controller choosing, delete or return all personal and other data to the Controller upon completion of the processing services and return any existing copies of the data, unless Swiss or agreed Cantonal law requires that the personal data be stored for a longer duration;

10. Make available to the Controller all information necessary to demonstrate compliance with its obligations and allow and cooperate fully with audits, including inspections, conducted by the Controller or another person authorised to this end by the Controller.

Preamble

This DPA details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Company as a data controller, and described in detail in the Beekeeper SaaS Subscription Agreement as signed respectively between the two Parties (hereinafter, the "Agreement"). Its regulations shall apply to any and all activities associated with the Agreement, in whose scope Processor's employees or agents process Company's personal data (hereinafter, "Data") on behalf of Company as a controller (hereinafter, "Contract Processing").

§ 1 Duration and specification of contract processing of Data

The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. Specifically, Contract Processing shall include, but not be limited to, the Data as declared in **Annex 1** of this DPA.

§ 2 Scope of application and responsibilities

1. The Processor shall act exclusively on documented instructions or service agreements from the Company. The Processor shall ensure that the Company Data entrusted is not used for other purposes or processed in any other way or form than as stated in the Company instructions, including transfer of Company Data to a third country or an international organisation.

2. Processor shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work. Company shall be solely responsible for compliance with the applicable statutory

requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Processor and the lawfulness of having Data processed on behalf of Company. Company shall be the »controller«.

3. The Processor shall process the Company Data in accordance with the law in force at any time. If the Processor deems an instruction to be in breach of such legislation, the Processor shall promptly inform the Company accordingly. However, this shall not apply if the law in question prohibits such notification for reasons of substantial public interest.

4. The Processor may not process the Company Data (including Personal Data) for any purpose other than instructed, unless the Processor is obliged to do so under the Swiss FADP, or agreed Cantonal data processing law as applicable. If so, the Processor shall notify the Company of such legal obligation **before** commencing the processing.

§ 3 Processor's obligations

1. For the performance of the obligations in relation to this Data Processing Agreement, the Processor shall only appoint such employees who were informed about all relevant data privacy obligations and instructed to comply with data secrecy pursuant to the Swiss Data Protection Act prior to performing their duties. The employees shall be sufficiently trained in order to be able to comply with their data protection and commercial contractual obligations. The Processor shall ensure an adequate level of training by implementing suitable controls. The Processor shall use additional means such as background checks of respective employees, where deem as an appropriate mitigating measure to any operational risk imposed on the Company.

2. Except where expressly permitted by the agreement, Processor shall process data subjects' Data only within the scope of the statement of work and the instructions issued by Company within the Agreement or this DPA. Where Processor believes that an instruction would be in breach of applicable law, Procesor shall notify Company of such belief without undue delay. Processor shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

3. Processor shall, within Processor's scope of responsibility, organise Processor's internal organisation so it satisfies the specific requirements of data protection.

Processor shall implement technical and organisational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the Swiss FADP and specifically its Section 2 Art. 7. Processor shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.

4. Processor reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

5. Processor shall support Company, insofar as is agreed upon by the parties, and where possible for Processor, in fulfilling data subjects' requests and claims.

6. Processor warrants that all employees involved in Contract Processing of Company's Data and other such persons as may be involved in Contract Processing within Processor's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Processor warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.

7. Processor shall notify Company, without undue delay, if Processor becomes aware of breaches of the protection of personal data within Processor's scope of responsibility.

8. Processor shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Processor shall coordinate such efforts with Company without undue delay.

9. Processor shall notify the Company point of contact (Annex 1) for any issues related to data protection arising out of or in connection with the Agreement.

10. Processor warrants that Processor fulfills its obligations to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

11. Processor shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible. Where an erasure, consistent

with data protection requirements, or a corresponding restriction of processing is impossible, Processor shall, based on Company's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material.

12. Processor shall, unless requested otherwise in writing at the time of termination by Company, upon termination of Contract act in accordance to the Term and Termination Clause of the Agreement.

13. Company shall bear any extra cost caused by deviating requirements in returning or deleting data.

14. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller. The record shall include the following:

- The name and contact information of the specific Processor, any sub-processor of the Commercial Contract (Beekeeper Software as a Service Subscription Agreement), the Company, the Data Protection Officer and, where relevant, the representative of the Processor.
- The categories of processing carried out by the Processor or any sub-processor on behalf of the Company.
- General description of the technical and organizational security measures undertaken by the Processor to safeguard the Company Data.

15. The list shall be in writing, including in electronic format. At the request of the Company, the Processor shall at any time make the list available to the Company.

16. When the processing of Company Data at the Processor takes place in home offices, in whole or in part, the Processor shall lay down guidelines for the personnel's processing of Company Data in home offices. The guidelines shall be submitted to the Company upon request.

17. The Processor shall participate in discussions, if any, with the Company and/or the Data Protection Agency and in good faith consider any recommendations and/or improvement notices, etc., from the Company and/or Data Protection Agency regarding the processing of Company Data.

18. The Processor shall promptly inform the Company if the Data Protection Agency contacts the Processor regarding the support or services covered by the DPA.

19. The Processor furthermore undertakes to promptly notify the Company of:

- Any request by a public authority for transfer of Company Data covered by the Commercial Contract, unless the notification of the Company is explicitly prohibited by law, e.g. pursuant to rules designed to ensure the non-disclosure of investigations performed by a law-enforcement authority.
- Any request for access received directly from the data subject or from another party.

§ 4 Company's obligations

1. Company shall notify Processor, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Processor's work.

2. Company shall notify to Processor the point of contact for any issues related to data protection arising out of or in connection with the Agreement in Annex 1 of this DPA.

3. In regards to compliance with the protective measures and safeguards outlined in **Annex 2** of this DPA, Processor agrees to maintain an Information Security Management System in accordance to ISO 27001:2013 Control Objectives and its verified effectiveness, parties refer to the existing certification issued and available to Company upon request as proof of the appropriate guarantees. Company is familiar with the technical and organisational measures of an ISMS as outlined by the Processor, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk.

§ 5 Enquiries by data subjects

1. Where a data subject asserts claims for rectification, erasure or access against Processor, and where Processor is able to correlate the data subject to Company, based on the information provided by the data subject, Processor shall refer such data subject to Company.

2. Processor shall forward the data subject's claim to Company without undue delay.

3. Processor shall support Company, where possible, and based upon Company's instruction insofar as agreed upon.

4. Processor shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

§ 6 Documentation

1. Processor shall document and prove to Company, Processor's compliance with the obligations agreed upon in this exhibit by appropriate measures.

2. Where specific types of documentation and proof can be identified, with regard to compliance with the obligations agreed upon, Processors may make available to Company the following information:

    - Conducting an own self-audit or self-assessment
    - Internal compliance regulations including external proof of compliance with these regulations
    - Certifications on data protection and/or information security (e.g. ISO 27001) ● Annual Penetration Test report performed by an external company
    - Any technical and/or organizational information deemed as necessary by the Company, **excluding** any information that may potentially, however remote, impact the security and/or confidentiality of another Customer or Supplier of Processor.

§ 7 Right to Audit and Inspection

1. The Company has the right to monitor the technical and organizational measures taken by the Processor at any time.

2. Where, in individual cases, audits and inspections to monitor the technical and organizational measures by Company or an auditor appointed by Company are necessary, such audits and inspections will require written confirmation from Processor, be conducted during regular business hours, and without interfering with Processor's operations, upon prior notice, and observing an appropriate notice period.

3. Processor may also require the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and

organisational measures and safeguards implemented.

4. Processor shall be entitled to rejecting auditors which are competitors of Processor.

5. Processor shall be entitled to request a remuneration for Processor's support in conducting inspections.

6. Processor's time and effort for such inspections shall be limited to one visit per calendar year, maximum of three days, unless agreed upon otherwise.

7. Company is fully responsible for any external incurred costs by Processor for such an audit or inspection.

8. Physical Access to Data Center locations of the Processor, is excluded from any such audit or inspection.

9. Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 1-6 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 8 Subprocessors (further processors on behalf of Company)

1. Processor shall use subprocessors as further processors on behalf of Company.

2. Subprocesses are only those as declared in this DPA **Annex 1** or where approved in advance by Company.

3. A subprocessor relationship shall be subject to such consent of Processor commissioning subprocessors with the performance agreed upon in the Agreement, in whole or in part.

4. Processor shall conclude, with such subprocessors, the contractual instruments necessary to ensure an appropriate level of data protection and information security and in line with the applicable data protection regulations.

5. Processor will conduct the Software as a Service (SaaS) performance listed in the Agreement, using third party service providers as listed in the **Beekeeper 3rd Party Use Statement** Declaration Form**.**

6. The term **'third party' means** a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal

data.

7. Save for the Infrastructure as a Service (IaaS) providers used for Data Center services and any other subprocessors declared in Annex 1 of this DPA, any new or change of third party service provider listed in the Beekeeper 3rd Party Use Statement Declaration Form **is not** considered as a change to or a new subprocessor, and use

thereof not subject to Company consent, agreement or notification for any reason whatsoever.

8. Processor is responsible to ensure any use of third party service providers is done legally and in the definition of the applicable requirements and framework of the agreed upon data protection legislation.

9. Processor shall obtain Company's consent prior to the use of new or replacement of existing subprocessors .

10. Company shall be entitled to contradict any change in a written notification by Processor for materially important reasons related to statutory data protection regulations or due to Company risk as a result of competitive disadvantage.

11. Processor must notify Company six (6) months prior to commencement of use of new or replacement subprocessor. Notification must be in writing.

12. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change.

13. Where a materially important reason for such contradiction exists, and failing an amicable resolution of this matter by the parties, both Company and Processor shall be entitled to terminate the Agreement and this DPA, to become effective for the commencement date of the use of the new or replacement subprocessor.

14. Where Processor commissions subprocessors, Processor shall be responsible for ensuring that Processor's obligations on data protection resulting from the Agreement and this DPA are valid and binding upon subprocessor.

15. Any costs of the establishment of an agreement with a subprocessor or a third party, including costs in connection with the drawing up of subprocessing agreements, shall be borne by the Processor and shall be of no concern to the Company.

16. The fact that the Company has consented to the Processor entering into an agreement with another subprocessor shall be of no consequence to the Processor's obligation to comply with this Data Processing Agreement.

§ 9 Company Data Breach Management and Notification

1. A “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2. The Processor shall inform the Company immediately and in writing of any personal data breach on Processing of Personal OR Company Data as stated in this Data Processing Agreement.

3. The Processor shall be obliged to provide the Company with any and all information necessary for the compliance with the Company obligations pursuant to the Swiss Data Protection Act on Processing of Personal Data or the Personal Data Protection regulation of any other applicable Canton.

4. The Processor shall then without undue delay, but not later than 72 hours after the personal data breach, report to the Company.

5. Processor shall notify the Company of the background of the security breach and the extent thereof as well as information about initiatives to safeguard against future security breach.

For Clarity & Transparency:

For the purpose of removing any assumptions, a reportable successful breach is one that is defined as "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons".

- In case of a successful breach where the Personal OR Company Data is impacted, the Processor will inform the Company immediately and no later than 72 hours.

§10 Technical and organizational measures

1. To ensure the protection of the Company Data and in order to comply with Personal Data laws and regulations, the Processor shall take the technical and

organizational measures necessary.

2. The Processor must implement and thus safeguard the Company Data with the necessary technical and organizational measures (inter alia with regard to storage, computing, networking access, transfer, input, order and availability control). Protective measures include using state-of-the-art software, computers and encryption methods as well as the use of adequate access controls for authentication and authorization (eg. two factor authentication and four eye control for authorization processes), password procedures, logging and documentation of processes and the implementation of a data security concept in accordance to measures outlined in the Processor's Security White Paper.

3. The measures taken shall be adequate for the protection of the specific Company Data, and protect against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in breach of the law in force at any time, including but not limited to the Swiss Data Protection Act on Processing of Personal Data or any agreed upon Cantonal requirements. This shall also apply if the processing of Company Data takes place, in whole or in part, in home offices.

4. If the Processor is established in another CH Canton, the Processor shall comply with both the security requirements laid down in applicable law in the place of operations for the Company and the security requirements laid down in the Canton or Jurisdiction of the Processor. On transferring the Company Data, electronically transmitted Company Data or Company Data made available for download shall be secured against unauthorized access.

§11 Transfer of Company Data

The Processor may not transfer or authorize the transfer of Company Data to countries outside the agreed and communicated jurisdiction(s) in the Agreement and this DPA with the Company.

§12 Duty of confidentiality

1. The Processor and the Processor's personnel shall observe unconditional confidentiality as regards the processing of Company Data, and the Processor and the Processor's personnel are thus only entitled to process Company Data in the performance of the Commercial Contract, including this DPA.

2. The Processor warrants that the Processor's personnel and any other subprocessor and the personnel of such other data processor who are authorized to process Company Data under this Data Processing Agreement will be subject to the duty of confidentiality as regards to Company Data which may come to their knowledge in connection with the performance of the Contract.

§13 Return and deletion of the Company Data upon cancellation and termination

Subject to the **Term and Termination** Clause of the Agreement, or upon written instruction by the Company and pursuant to the relevant provisions of statutory law and regulations, the Processor shall facilitate the correction, deletion and blocking of Company Data processed on behalf of the Company until these Company Data are ultimately deleted in accordance to the Agreement.

§14 Duration

1. The Data Processing Agreement shall enter into force upon signature thereof and shall remain in force for as long as the Processor processes on behalf of the Company, or until the Agreement expires/terminates, whichever is later.

2. Upon expiration or termination of the Data Processing Agreement, regardless of the legal reasons for the termination, the Processor shall provide the necessary services to the Company in accordance with para. 3 of the DPA.

§15 Obligations to inform, mandatory written form, choice of law

1. Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by outside parties while in Processor’s control, Processor shall notify Company of such action without undue delay. Processor shall, without undue delay, notify all pertinent parties in such action, that any data affected thereby is in Company’s sole property and area of responsibility, that data is at Company’s sole disposition, and that Company is the responsible body.

2. No modification of this annex and/or any of its components – including, but not limited to, Processor’s representations and warranties, if any – shall be valid and binding unless made in writing, and furthermore only if such modification expressly

states that such modification applies to the regulations of this DPA. The foregoing shall also apply to any waiver or modification of this mandatory written form.

3. In case of any conflict, the data protection regulations of this DPA shall take precedence over the regulations of the Agreement. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

4. The Applicable Law and Jurisdiction for this DPA is the same as the Agreement.

§16 Liability and damages

Liabilities and damages for this DPA is in the first instance what may be defined and as that set by a court of law and in the absence or agreement to exclude the first instance will be in accordance to the liability and damages set in the Agreement.

§17 Precedence

In the event of any discrepancy between the terms of this Data Processing Agreement and any other agreement between the Parties, whether in writing or oral, including the Commercial Contract, the requirements set forth in the Swiss Data Protection Act for Company Data processed in Switzerland as enforced at the time for all other jurisdictions shall determine the requirements for precedence.

§18 Counterparts and Electronic Signatures

The Data Processing Agreement shall be signed in two original copies, of which the Parties shall each receive one. This DPA may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Photographic, electronic PDF, and facsimile copies of such signed counterparts may be used in lieu of the originals for any purpose. The authorized signatures below may be electronic signatures in conformity with local legal practice.

ANNEX 1

Description of the Transfer and Processing

1. Catalogue [and classification of sensitivity] of Personal Data to be transferred and processed:

2. Purpose(s) of the transfer and processing:

3. Categories of Persons Affected:

4. Persons who may access or receive the Personal Data:

Note: Subcontractors OR Subprocessors are not equal or the same as third party companies, as described in the Beekeeper "3rd Party Use Statement Declaration Form." This DPA is applicable to Subcontractors and Subprocessors only.

Subcontractor/Subprocessor (name, legal status, place of business)	Processing Jurisdiction	Type of service (IaaS) Infrastructure as a Service = Data Center Services = BCP/DR Solutions for Database and Cryptographic services

5. Additional useful information (Any agreed definitions may be stated here):

6. Contact Information for Data Protection Inquiries (Data Protection Officer):

BEEKEEPER **Data Protection Officer**	**Dr. Amir Ameri**	**Contact Number** amir@beekeeper.io dpo@beekeeper.io

ANNEX 2

Technical and Organizational Measures implemented by the Processor

Documentation of the technical and organizational measures to be implemented by the processor for the proper fulfilment of the service provided .

Note: The processor is allowed to update the technical and organizational measures to the state of the art, without reducing the data protection level.

Description of the measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(1) Measures for pseudonymisation and encryption of personal data

With the current service and product offerings, as we do not process any data outside of the product platform limited to data storage, we do not utilize pseudonymisation measures. We do encrypt data, including Personal Data where available, as defined in our Security White Page. In short encryption is utilized for storage of data on the mobile devices. Our DB hosted in our VPC in all our Data Centers are encrypted. In practice, only encrypted links are used as Transfer channels. Please refer to our Security White Paper.

(2) Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services:

We have implemented a number of measures to safeguard the confidentiality, integrity, availability and resilience of the service offering, as listed below:

1. An Information Security Management System (ISMS) Certified in accordance to ISO 27001:2013 Control Objectives.
2. Embedded Governance structure for Operational Risk Management. This includes a comprehensive Operational Risk Management process, including BERI (Beekeeper Risk Inventory).
3. Use of two factor authentication for all employees.
4. Secure workplace solution accordingly with notebooks that are encrypted and anti virus protected.
5. Implementation of a VPC (Virtual Private Cloud) with limitation to 1 jurisdiction of choice by the Data Controller. All Data Center partners hold ISO 27001 Certification among other requirements.
6. Protection of the VPC environment with a segregated security architecture including border firewalls controlled fully by Beekeeper employees. (Security White Paper)

7. Limited access to production tenant for authorized Beekeeper employees based on the

Beekeeper Information Security Policy for Customers.

8. No permanent access to production environment, other than individuals defined in 6 above. 9.

Governance of authorization for access based on “Need to Do---Need to Access” Principle. 10.

Control Process for access to production tenant by defined Customer Support Manager.

11. Control Process for access to production for engineering support based on a limited time (1 hour) issued certificate from a VPN with alerting for issuance of the certificate.

12. Separation of access for Production, Staging and Development environment.

13. Provisioning of Dashboard functionalities for complete onsite user management by the Data Controller.

14. Provisioning of direct interface to SSO or AD or SFTP solutions for management of authorized users for access. (if deployed by Controller)

15. Use of the push principle when utilizing any 3rd party service (they cannot initiate data pull).

16. Defined 3rd Party Assessment Policy (attached)

17. Defined and controlled Change Management Process based on Submitter / Reviewer / Approver & Implementer. High level of automated in a Microservices environment.

18. Encrypted communication based on TLS 1.2 with daily certificate verification

19. Adequate Logging of access to Beekeeper Production environment

20. Defined controlling measures by Risk and Compliance

21. Continuous training and awareness seminars for all Beekeeper employees, part time/full time/contractors:

    a. Mandatory sessions per year

    b. Engineering specific sessions under Secure Coding monthly

    c. Special Information Security session offered monthly for new joiners

22. Use of High Resilience offered Backup and Data Recovery solution

23. Online monitoring of service availability and subscription is available to the Controller (status.beekeeper.io)

24. Contractually binding service availability commitment for 99.9%

(3) Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Beekeeper as a company performs Quarterly Scenario based Business Continuity and Disaster Recovery Tests, as defined in the BCP / DR Policy for Beekeeper.

(4) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing:

Risk Management Governance structure with the following scope:

1. Weekly and Quarterly Risk Meeting between Engineering and Risk & Compliance 2.

Maintaining a Risk Profile by entering all identified operational Risks in BERI, see (2)2 3.

Annual Penetration Testing by an External Company

4. On demand Penetration Testing by Customers

5. Continuous Security Vulnerability Scanning of the code base

6. Testing and Quality Assurance incorporated in the Change Management process

7. Annual 3rd Party Risk Assessment as applicable according to Beekeeper 3rd Party Assessment Policy.

8. Defined Security Incident Management Policy

9. Defined Security Incident Notification Policy and Process.

10. Performance of internal assessments according to ISO 27001 Control Objectives by a Certified ISO 27001 Internal Auditor.

(5) Our Vulnerability Management Program and respectively Policy consists of the following:

a. Daily (upon code change) code base scanning using Quays Security Scanner

b. Daily scanning of our certificates using Qualys Security Scanner

c. NIDS + HIDS monitoring by both ourselves and our IaaS providers

d. External full scope annual penetration tests (APPS and network and architecture) e.

A Risk Management process to manage the Vulnerability found, assigned, etc.

***