Data Processing Addendum

This Alcatraz AI, Inc. (“Alcatraz”) Data Processing Addendum and its Annexes (“DPA”) reflects the parties’ agreement regarding the Processing of Personal Data by Alcatraz on behalf of System Owner (might be referred also as Solution Owner, Client, Customer) in connection with Alcatraz’s Services under the customer Agreement between System Owner, and Alcatraz (also referred to in this DPA as the “Agreement”).

This DPA is supplemental to and forms an integral part of the Agreement. In case of any conflict or inconsistency with the Agreement, this DPA will take precedence over the Agreement to the extent of such conflict or inconsistency.

Alcatraz updates the terms of this DPA from time to time. Alcatraz informs customers with an active subscription when an update is available via email or through an Authorized Channel Partner. Archived versions of the DPA can be accessed in our archives on our website under Legal.

1. DEFINITIONS

Terms not otherwise defined in this DPA have the meaning as outlined in the Agreement.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

Data Protection Laws: All applicable worldwide legislation relating to data protection and privacy that applies to the respective party in the role of Processing Personal Data in question under the Agreement.

Data Subject: The individual to whom Personal Data relates.

Instructions: The written or documented instructions issued by a Controller to a Processor and directing the same to perform a specific or general action regarding Personal Data (including, but not limited to, depersonalizing, blocking, deletion, and providing of Personal Data).

Permitted Affiliates: means any companies controlling, being controlled by, or under common control with the party whether directly or indirectly.

Personal Data: means any information which alone or in combination with other information can be used to identify a living person and is Processed by Alcatraz on behalf of System Owner, Personal Data can include, but not limited to:
a. Biometric data, which is a unique encrypted binary number representing a combination of unique points from the customer’s face. This data is stored in an encrypted format and cannot be used to recreate your facial image. b. Badge Number for identification purposes within the platform.

Personal Data Breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted.

Processing: Any operation or set of operations which is performed on Personal Data, including storage, use, access and reading. The terms “Process,” “Processes,” and “Processed” will be construed accordingly.

Processor: A natural or legal person, public authority, agency, or other body that Processes Personal Data on behalf of the Controller.

Sub-Processor: Any Processor engaged by Alcatraz or our Affiliates to assist in fulfilling our obligations concerning the provision of the Services under the Agreement. Sub-processors may include third parties or Alcatraz Affiliates but will exclude any Alcatraz employee or consultant.

System Owner: The customer who enters into an Agreement with Alcatraz or an Alcatraz Partner to install, operate, and license the Rock. Depending on the relevant Agreement might be referred as Solution Owner, Client, Customer or equivalent.

2. ROLES OF THE PARTIES

2.1. When Processing Personal Data under System Owner Instructions, the parties acknowledge and agree that System Owner is acting as the Controller of Personal Data (either as the Controller or as a Processor on behalf of another Controller) and Alcatraz is the Processor under the Agreement.

3. SYSTEM OWNER RESPONSIBILITIES

3.1. **Compliance with Laws.** System Owner must comply with all laws and regulations applicable to the use of Alcatraz's services, including laws related to biometric data, confidentiality of communications, and Data Protection Laws. In particular but without prejudice to the generality of the foregoing, System Owner acknowledge and agree that System Owner will be solely responsible for: (i) the accuracy, quality, and legality of its data and the means by which System Owner acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations; (iii) ensuring System Owner have the right to transfer, or provide access to, the Personal Data to Alcatraz for Processing under the terms of the Agreement (including this DPA); (iv) System Owner will inform Alcatraz without undue delay if System Owner is not able to comply with its responsibilities under this 'Compliance with Laws' section.

3.2. **Controller Instructions.** The parties agree that the Agreement (including this DPA), together with System Owner use of the service under the Agreement, are System Owner's complete Instructions to Alcatraz about the Processing of Personal Data.

3.3. **Security.** System Owner is solely responsible for making an independent determination as to whether the technical and organizational measures for Services described in Annex 2 meet System Owner requirements, including any of System Owner security obligations under applicable Data Protection Laws.

4. ALCATRAZ AI OBLIGATIONS

4.1. **Compliance with Instructions.** Alcatraz will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of System Owner lawful Instructions, unless and to the extent otherwise required by applicable law. Alcatraz is not responsible for compliance with any Data Protection Laws applicable to System Owner or System Owner industry that are not applicable to Alcatraz.

4.2. **Conflict of Laws.** If Alcatraz learns that Alcatraz cannot Process Personal Data under System Owner instructions due to a legal requirement under any applicable law, Alcatraz will (i) promptly inform the System Owner about that legal requirement to the extent allowed by the applicable law; and (ii) where necessary, stop all Processing (other than merely storing and maintaining the security of the affected Personal Data) until System Owner issue new Instructions with which

Alcatraz can comply. If this provision is invoked, Alcatraz will not be liable to System Owner under the Agreement for any failure to perform the applicable services.

4.3. **Security.** Alcatraz will implement and maintain technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, Alcatraz may modify or update the Security Measures at our discretion if the modification or update does not result in a material degradation in the protection offered by the Security Measures.

4.4. **Confidentiality.** Alcatraz will make sure any staff whom Alcatraz authorizes to Process Personal Data is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) concerning that Personal Data.

4.5. **Personal Data Breaches.** Alcatraz will inform System Owner without undue delay after Alcatraz becomes aware of any Personal Data Breach and will assist System Owner.

4.6. **Deletion or Return of Personal Data.** Alcatraz will delete or return all System Owner's data, including Personal Data (including copies thereof) Processed under this DPA, as per System Owner's instructions or should System Owner discontinue using Alcatraz's services unless required otherwise by applicable law.

5. DATA SUBJECT REQUESTS

5.1. The Alcatraz platform provides System Owner with several controls that System Owner can use to retrieve, correct, delete, or restrict the Processing of Personal Data, which System Owner can use to assist it in connection with System Owner obligations under Data Protection Laws, including System Owner obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

5.2. If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Alcatraz, Alcatraz will promptly inform System Owner and advise the Data Subject to submit their request to System Owner. System Owner will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

6. SUB-PROCESSORS

6.1. System Owner agrees Alcatraz may engage Sub-Processors to Process Personal Data on System Owner's behalf, and Alcatraz does so in three ways. First, Alcatraz may engage Sub-Processors to assist Alcatraz with hosting and infrastructure. Second, Alcatraz may engage with Sub-Processors to support product features and integrations. Third, Alcatraz may engage with Alcatraz Affiliates as Sub-Processors for service and support.

6.2. Alcatraz has appointed, as Sub-Processors, the third parties and Alcatraz Affiliates listed in Annex 3 to this DPA.

6.3. Alcatraz will allow System Owner to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 30 days of receipt of notification of change. Should System Owner object to the engagement of a new Sub-Processor, Alcatraz, and System Owner will discuss System Owner concerns in good faith to achieve a commercially reasonable resolution. If no such resolution can be reached, Alcatraz will, at its sole discretion, either not appoint the new Sub-Processor, or permit System Owner to suspend or terminate the affected service under the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by System Owner before suspension or termination).

6.4. Where Alcatraz engages Sub-Processors, Alcatraz will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors.

7. DEMONSTRATION OF COMPLIANCE

7.1. Alcatraz will make all information reasonably necessary to demonstrate compliance with this DPA available to System Owner and allow for and contribute to audits, including inspections conducted by System Owner or System Owner auditor to assess compliance with this DPA, where required by applicable law. System Owner acknowledges and agrees that System Owner will exercise System Owner audit rights under this DPA by instructing Alcatraz to comply with the audit measures described in this 'Demonstration of Compliance' section. System Owner acknowledges that the Service is hosted by our hosting Sub-Processors who maintain independently validated security programs and that Alcatraz's systems are audited annually as part of security compliance and regularly tested by independent third-party penetration testing firms. Upon request, Alcatraz will supply (on a confidential basis) recent certifications and/or summary audit reports to System Owner so that System Owner can verify Alcatraz's compliance with this DPA. Further, at System Owner's written request, Alcatraz will provide written responses (on a confidential basis) to all reasonable requests for information made by System Owner necessary to confirm our compliance with this DPA, provided that System Owner will not exercise this right more than once per calendar year unless System Owner has reasonable grounds to suspect non-compliance with the DPA. This Section 7.1 will not affect System Owner's statutory audit rights under Article 28 of the GDPR.

8. TRANSFER MECHANISM FOR DATA TRANSFERS

8.1. Alcatraz will not transfer Personal Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws) unless it first takes all such measures as are necessary to ensure the transfer complies with applicable European Data Protection Laws. Such measures may include (without limitation) (i) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including the Data Privacy Framework; (ii) to a recipient that has achieved binding corporate rules permission under European Data Protection Laws; or (iii) to a recipient that has executed the Standard Contractual Clauses in each case as adopted or approved under applicable European Data Protection Laws.

8.2. To the extent that Alcatraz receives European Data in the United States in connection with the performance of the Services, Alcatraz will follow:

A. Data Privacy Framework. Alcatraz will use the Data Privacy Framework to lawfully receive European Data in the United States and make sure it provides at least the same level of protection to such European Data as is required by the Data Privacy Framework Principles and will notify System Owner in writing if it is unable to comply with this requirement.

B. Standard Contractual Clauses. If European Data Protection Laws require that safeguards are put in place (for example, if the Data Privacy Framework does not cover the transfer to Alcatraz and/or the Data Privacy Framework is invalidated), the Standard Contractual Clauses will be incorporated by reference s available on the EU Commission website , and form part of the Agreement:

(a) In relation to European Data subject to the GDPR (i) System Owner are the "data exporter" and Alcatraz is the "data importer"; (ii) the Module Two terms apply to the extent the System Owner are a Controller of European Data and the Module Three terms apply to the extent the System Owner are a Processor of European Data; (iii) in Clause 7, the optional docking clause applies; (iv) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified under the 'Sub-Processors' section of this DPA; (v) in Clause 11, the optional language is deleted; (vi) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be determined under the 'Contracting Entity; Applicable Law; Notice' section of the Jurisdiction Specific Terms or, if this section does not

specify an EU Member State, the Republic of Ireland (without reference to conflicts of law principles); (vii) the Annexes of the Standard Contractual Clauses will be considered completed with the information set out in the Annexes of this DPA; (viii) the supervisory authority that will act as competent supervisory authority will be determined under GDPR; and (ix) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA the Standard Contractual Clauses will prevail for such conflict.

(b) In relation to European Data subject to the UK GDPR, the Standard Contractual Clauses will apply under sub-section (a), and these modifications (i) the Standard Contractual Clauses will be changed and interpreted under the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be considered completed with the information set out in the Annexes of this DPA and Table 4 will be considered completed by selecting "neither party"; and (iii) any conflict between the Standard Contractual Clauses and the UK Addendum will be resolved under Section 10 and Section 11 of the UK Addendum.

(c) In relation to European Data subject to the Swiss DPA, the Standard Contractual Clauses will apply under subsection (a), and these modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner" and the "relevant courts in Switzerland."

(d) System Owner agrees that by meeting our obligations under the 'Sub-Processors' section of this DPA, Alcatraz fulfills its obligations under Section 9 of the Standard Contractual Clauses. For Clause 9(c) of the Standard Contractual Clauses, System Owner acknowledges that Alcatraz may be restricted from disclosing Sub-Processor agreements, but Alcatraz will use reasonable efforts to require any Sub-Processor Alcatraz appoint to permit it to disclose the Sub-Processor agreement to System Owner and will provide (on a confidential basis) all information Alcatraz reasonably can. System Owner also agrees that System Owner will exercise System Owner audit rights under Clause 8.9 of the Standard Contractual Clauses by instructing Alcatraz to follow the measures described in the 'Demonstration of Compliance' section of this DPA.

(e) Where the Alcatraz contracting entity under the Agreement is not Alcatraz, this contracting entity (not Alcatraz) will remain fully and solely responsible and liable to System Owner for the performance of the Standard Contractual Clauses by Alcatraz and System Owner will direct any instructions, claims, or inquiries concerning the Standard Contractual Clauses to this contracting entity. If Alcatraz cannot meet its obligations under the Standard Contractual Clauses or is In breach of any warranties under the Standard Contractual Clauses or UK Addendum for any reason, and System Owner intends to suspend the transfer of European Data to Alcatraz or terminate the Standard Contractual Clauses, or UK Addendum, System Owner agree to give Alcatraz reasonable notice to enable Alcatraz to cure this non-compliance and reasonably cooperate with Alcatraz to identify what additional safeguards may be implemented to remedy this non-compliance. If Alcatraz has not or cannot cure the non-compliance, System Owner may suspend or terminate the affected part of the Service under the Agreement without liability to either party (but without prejudice to any fees System Owner has incurred before this suspension or termination).

8.3. **Alternative Transfer Mechanism.** If Alcatraz must adopt an alternative transfer mechanism for European Data, in addition to or other than the mechanisms described in sub-section (B) above, such alternative transfer mechanism will apply automatically instead of the mechanisms described in this DPA (but only to the extent such alternative transfer mechanism follows with European Data Protection Laws), and System Owner

agrees to execute such other documents or take such action as may be reasonably necessary to give legal effect such alternative transfer mechanism.

9. MORE PROVISIONS FOR CALIFORNIA PERSONAL INFORMATION

9.1. **Scope.** The 'Additional Provisions for California Personal Information' section of the DPA will apply only to California Personal Information.

9.2. **Roles of the Parties.** When processing California Personal Information under System Owner Instructions, the parties agree that System Owner is a Business, and Alcatraz is a Service Provider for the CCPA.

9.3. **Responsibilities.** Alcatraz certifies that Alcatraz will Process California Personal Information as a Service Provider strictly to perform the Services and Consulting Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA, including as described in the 'Usage Data' section of our Privacy Policy. Further, Alcatraz certifies Alcatraz (i) will not Sell or Share California Personal Information; (ii) will not Process California Personal Information outside the direct business relationship between the parties, unless required by applicable law; and (iii) will not combine the California Personal Information in Customer Data with personal information Alcatraz collect or receive from another source (other than information Alcatraz receive from another source in connection with our obligations as a Service Provider under the Agreement).

9.4. **Compliance.** Alcatraz will (i) meet obligations applicable to Alcatraz as a Service Provider under the CCPA and (ii) give California Personal Information with the same level of privacy protection as required by the CCPA. Alcatraz will tell System Owner if Alcatraz decides that Alcatraz can no longer meet our obligations as a Service Provider under the CCPA.

9.5. **CCPA Audits.** System Owner will have the right to take reasonable steps to help make sure that Alcatraz uses California Personal Information in a way consistent with the System Owner's obligations under the CCPA. Upon notice, System Owner will have the right to take reasonable steps under the Agreement to stop and remedy unauthorized use of California Personal Information.

9.6. **Not a Sale.** The parties agree that the disclosure of California Personal Information by the System Owner to Alcatraz does not form part of any monetary or other valuable consideration exchanged between the parties.

10. GENERAL PROVISIONS

10.1. **Amendments.** Despite anything to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, Alcatraz reserves the right to make any updates and changes to this DPA and the terms that apply in the 'Amendment; No Waiver' section of the General Terms will apply.

10.2. **Severability.** If any individual provisions of this DPA are found to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

10.3. **Limitation of Liability.** Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (including any other DPAs between the parties) and the Standard Contractual Clauses, where applicable, whether in contract, tort, or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the Agreement and any reference in this section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA). To avoid doubt, if Alcatraz is not a party to the Agreement, the 'Limitation of Liability' section of the Agreement will apply as between System Owner and Alcatraz, and in this respect, any references to 'Alcatraz', 'we', 'us' or 'our' will include both Alcatraz and the Alcatraz entity that is a party to the Agreement. In no event will either party's liability be limited regarding any

individual's data protection rights under this DPA (including any other DPAs between the parties and the Standard Contractual Clauses, where applicable) or otherwise.

10.4. **Governing Law.** This DPA will be governed by and construed under the Contracting Entity, Applicable Law; Notice sections of the Jurisdiction Specific Terms, unless required otherwise by Data Protection Laws.

11. PARTIES TO THIS DPA

11.1. **Permitted Affiliates.** By signing the Agreement, System Owner enters into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of System Owner and in the name and on behalf of System Owner Permitted Affiliates. For this DPA only, and unless indicated otherwise, the terms "Customer," and "System Owner," will include System Owner and such Permitted Affiliates.

11.2. **Authorization.** The legal entity agreeing to this DPA as System Owner represents that it may agree to and enter into this DPA for and on behalf of itself and each of its Permitted Affiliates.

11.3. **Remedies.** The parties agree that (i) only the Customer entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement will exercise any rights like these under this DPA not separately for each Permitted Affiliate individually but in a combined way for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all Instructions, authorizations, and communications with Alcatraz under the DPA and will have the right to make and receive any communications related to this DPA on behalf of its Permitted Affiliates.

11.4. **Other rights.** The parties agree that System Owner will when reviewing our compliance with this DPA under the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on Alcatraz and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Permitted Affiliates in one audit.

The below Parties have read and agreed to the terms of this Agreement and, as duly authorized representatives, execute this Agreement as of the Effective Date.

Annex 1 – Parties and Transfers

A. List of Parties

Data exporter:

Name: The Customer, as defined in the Agreement (on behalf of itself and its Affiliates)

Address: The Customer's address, as set out in the Order Form

Contact person's name, position, and contact details: The Customer's contact details, as set out in the Order Form and/or as set out in the Customer's Alcatraz Account

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Alcatraz Services under the Alcatraz Customer Terms of Service

Role (controller/processor): Controller (either as the Controller; or acting in the capacity of a Controller, as a Processor, on behalf of another Controller)

Data importer:

Name: Alcatraz AI Inc.

Address: 10061 Bubb Rd. 300 Cupertino, CA 95014.

Contact person's name, position, and contact details: Annie Pratt, VP Operations, legal@alcatraz.ai.

Activities relevant to the data transferred under these Clauses:

Processing of Personal Data in connection with Customer's use of the Alcatraz Services under the Agreement

Role (controller/processor): Processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is Transferred

System Owner may submit Personal Data while using the Service, the extent of which is determined and controlled by System Owner in System Owner sole discretion, and which may include, but is not limited to Personal Data relating to these categories of Data Subjects:

System Owner contacts and other end users include System Owner employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors. Data Subjects may also include individuals trying to communicate with or transfer Personal Data to System Owner end users.

Categories of Personal Data

System Owner may submit Personal Data to the Services, the extent of which is determined and controlled by System Owner in System Owners sole discretion, and which may include but is not limited to these categories of Personal Data:

1. Distance between eyes
2. Width of nose
3. Distance between mouth and eyebrows.
4. Outline of nose
5. Outline of chin
6. Outline of jawline
7. Facial Geometry
8. Badge number
9. Name
10. E-mail address

Sensitive Data transferred and applied restrictions or safeguards.

Frequency of the transfer: Continuous

Nature of the Processing:

Personal Data will be Processed under the Agreement (including this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain, and improve the Services provided to System Owner and/or
2. Disclosure under the Agreement (including this DPA) and/or as compelled by applicable laws.

Purpose of the transfer and processing

Alcatraz will Process Personal Data as necessary to provide the Services under the Agreement, as further specified in the Order Form, and as further instructed by System Owner in System Owner use of the Services.

Period for which Personal Data will be retained:

Subject to the 'Deletion or Return of Personal Data' section of this DPA, Alcatraz will Process Personal Data during the Agreement unless otherwise agreed in writing.

Annex 2 – Security Measures

Alcatraz observes the Security Measures described in Annex 2. All capitalized terms not otherwise defined will have the meanings as stated in the General Terms. For more information on these security measures, please refer to Alcatraz's Security Overview and Penetration Test Summaries by contacting legal@alcatraz.ai.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Alcatraz hosts our Service with outsourced cloud infrastructure providers. Additionally, Alcatraz has contractual relationships with vendors, including, but not limited to, Amazon Web Services, to provide the Service under our DPA. Alcatraz relies on contractual agreements, privacy policies, and vendor compliance programs to protect data processed or stored by these vendors. The System Owner has the option to install the Service on the System Owner's premises, thereby eliminating the need for outsourced processing.

Physical and environmental security: Alcatraz hosts product infrastructure with multi-tenant, outsourced infrastructure providers. Alcatraz recognizes that some System Owners have specific compliance requirements or may prefer an even higher level of data isolation. For these customers, we offer a premium Single-Tenant Hosting option. The Single-Tenant Hosting option is available as a premium service upgrade. Alcatraz does not own or maintain hardware at the outsourced infrastructure providers' data centers. Production servers and client-facing applications are logically and physically secured from the internal corporate information systems. The physical and environmental security controls are currently audited for ISO 27001 compliance, among other certifications.

Authentication: Alcatraz implements a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing nonpublic customer data.

Permission: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The Permission model in each product is designed to make sure that only the appropriately assigned individuals can access relevant features, views, and customization options. Permission to data sets is performed by confirming the user's permissions against the attributes associated with each data set. Alcatraz maintains data segregation. Each System Owner's data set is logically separated and isolated from all other System Owner data sets. This segmentation ensures that one customer cannot access, view, or modify another customer's data under any circumstances.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth permission.

ii) Preventing Unauthorized Product Use

Alcatraz put industry standards into practice for access controls and detection capabilities for the internal networks that support our products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures put into practice differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignments, and traditional firewall rules.

Penetration testing: Alcatraz utilizes industry-recognized penetration testing service providers for penetration testing of both the Alcatraz web application and internal corporate network infrastructure at least yearly. These penetration tests intend to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees has permitted access to the products and to customer data via controlled interfaces only if the customer allows. The intent of providing access to a subset of employees is to provide effective customer support, product development, and research, troubleshoot potential problems, detect and respond to security incidents, and implement data security. Access is enabled through “just in time” (JITA) requests for access; all such requests are logged. Employees are granted access by role, and reviews of high-risk privilege grants are started daily. Administrative or high-risk access permissions are reviewed at least once every six months.

Background checks: Where permitted by applicable law, Alcatraz employees undergo third-party background or reference checks. In the United States, employment offers are dependent on the results of a third-party background check. All Alcatraz employees must conduct themselves in a way consistent with company guidelines, nondisclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Alcatraz requires HTTPS encryption (also called SSL or TLS) on all login interfaces and every customer site hosted on the Alcatraz products. Our HTTPS implementation uses TLS 1.2 industry-standard algorithms and certificates.

At-rest: Alcatraz stores user passwords following policies that follow industry-standard practices for security. Alcatraz has implemented technologies using AAES 256B encryption to ensure that stored data is encrypted at rest.

c) Input Control

Detection: Alcatraz designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert employees of malicious, unintended, or anomalous activities. Our staff, including security, operations, and support personnel, respond to known incidents.

Response and tracking: Alcatraz maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support staff; and resolution steps are identified and documented. For any confirmed incidents, Alcatraz will take steps to reduce product and Customer damage or unauthorized disclosure.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure at least 99.95% uptime. The providers maintain at least N+1 redundancy to power, network, and heating, ventilation, and air conditioning (HVAC) services.

Fault tolerance: For Cloud Services, backup and replication strategies are designed to ensure redundancy and failover protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where possible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry-standard methods.

Disaster Recovery Plans: Alcatraz maintains and regularly test disaster recovery plans to help ensure the availability of information following interruption to, or failure of, critical business processes. Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected to prevent single points of failure. This design helps our operations in maintaining and updating the product applications and backend while limiting downtime.

Annex 3–Sub-Processors

To help Alcatraz deliver the Cloud Service, Alcatraz engages Sub-Processors to help with our data processing activities.

A list of our Sub-Processors and our purpose for engaging them is on our Alcatraz web page, which is incorporated into this DPA.

Third-Party Sub-Processor, Country, website	Purpose
Amazon Web Services, USA https://aws.amazon.com/	Hosting and Infrastructure
A-LIGN Compliance and Security. Inc., USA https://www.a-lign.com/	Cybersecurity and compliance solutions provider
Asset Panda, USA https://www.assetpanda.com/	Cloud-based asset tracking and management solution
Atlassian, USA https://www.atlassian.com/	Team collaboration software
Channeltivity, USA https://www.channeltivity.com/	Partner Relationship Management software platform
Google Workspace, USA https://workspace.google.com/	Team collaboration software
HubSpot, USA https://www.hubspot.com/	HubSpot Solutions

OpenVPN, USA https://openvpn.net/	Network security company
Recapped. io, USA https://www.recapped.io/	Customer Collaboration Platform
Slack, USA https://slack.com/	Cloud-based team communication platform
Zoom, Israel https://www.zoom.com/	Online meeting application
Alcatraz Bulgaria EOOD 1 Mladost, ul. "Dimitar Mollov" 8, 1750 Sofia, Bulgaria	Affiliate of Alcatraz AI, Inc.

Due to the nature of our global business and our continuous commitment to ensuring customer satisfaction, our business needs and service providers may change occasionally. For example, Alcatraz might stop using a particular service provider to streamline and reduce the number of providers Alcatraz uses. But Alcatraz might bring in a new service provider if it will help Alcatraz provide a better Service.

System Owner may subscribe for email notifications when Alcatraz updates this page due to additions, replacements, or significant changes in services by Sub-Processors, including changes in their service location. To subscribe please contact legal@alcatraz.ai. If System Owner opt-ins to receive such an email, one will be provided at least 30 days before any change.

For more information on Alcatraz's privacy practices, please visit our Privacy Policy. If System Owner have questions regarding this page, please contact Alcatraz at legal@alcatraz.ai.