

Annex 2 Alcatraz's Technical and Organizational Measures

Alcatraz observes the Security Measures described in herein. 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 and SOC 2 Type II 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 or higher 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 AES 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.