Last update: October 26, 2021

ALTINITY.CLOUD

Data Processing Addendum

This Data Processing Addendum and its Appendixes ("**DPA**") forms part of, and is subject to, the Altinity.Cloud Terms of Service, or other written or electronic terms of service or subscription agreement between Altinity, Inc., a Delaware corporation, ("**Altinity**") and the legal entity defined therein as the "**Customer**" (the "**Agreement**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

This DPA reflects the parties' agreement with respect to the Processing of Personal Data by Altinity, on Customer's behalf, in connection with the Services provided in the Agreement.

In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

1. Definitions.

"**Account**" means Customer's account in the Service in which Customer stores and processes Customer Data.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Authorized Affiliate**" shall mean a Customer Affiliate that is permitted to use the Services pursuant to the Agreement, has not signed its own separate agreement with Altinity and are not a "Customer" as defined under the Agreement, and is either a Data Controller or Data Processor for the Customer Personal Data Processed by Altinity pursuant to the Agreement, for so long as such entity remains a Customer Affiliate.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended from time to time.

"**Customer Data**" has the meaning set forth in the Agreement.

"**Customer Personal Data**" means any Customer Data that is Personal Data.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU & UK Data Protection Law and the CCPA.

"**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

"**EU & UK Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") and (ii) the GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act of 2018 ("**UK GDPR**") and the Data Protection Act of 2018.

"**Personal Data**" means any information, including opinions, relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including, but not limited to, the definition of "personal information" in the CCPA.

"**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Purposes**" shall mean (i) Altinity's provision of the Services as described in the Agreement, including Processing initiated by Users in their use of the Services, and (ii) further documented, reasonable instructions from Customer agreed upon by the parties.

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

"**Services**" means the generally available Altinity software-as-a-service offering described in the Documentation and procured by Customer, and any other services provided by Altinity under the Agreement, including but not limited to support and technical services.

"**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries approved pursuant to Commission Decision (EU) 2021/914 of 4 June 2021, found at ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

"**Sub-processor**" means any other Data Processors engaged by Altinity to Process Customer Personal Data.

2. Scope and Applicability of this DPA.

This DPA applies where and only to the extent that Altinity Processes Customer Personal Data on behalf of Customer as Data Processor in the course of providing the Services.

3. Roles and Scope of Processing.

3.1 **Role of the Parties**. As between Altinity and Customer, Altinity shall Process Customer Personal Data only as a Data Processor (or sub-processor) acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein, in each case regardless of whether Customers acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller ("**Third-Party Controller**") with respect to Customer Personal Data. To the extent any Usage Data (as defined in the Agreement) is considered Personal Data under applicable Data Protection Laws, Altinity is the Data Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws.

3.2 **Customer Instructions**. Altinity will Process Customer Personal Data only for the Purposes. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out Customer's exclusive instructions to Altinity for the Processing of Customer Personal Data. Any Processing outside the scope of these instructions will require prior written agreement between Customer and Altinity. Altinity shall promptly notify Customer if, in Altinity's opinion, such an instruction violates EU & UK Data Protection Law. Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with a Third-Party Controller.

3.3 **Customer Affiliates.** Altinity's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to Section 11 (Parties to the DPA), and the following conditions:

(a) Customer must exclusively communicate any additional Processing instructions requested pursuant to Section 3.2 directly to Altinity, including instructions from its Authorized Affiliates; and

(b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer.

3.4 **Customer Processing of Personal Data**.

(a) Customer agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Customer Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing and backing- up Customer Personal Data; and (iii) has obtained all consents, permissions and rights necessary under Data Protection Laws for Altinity to lawfully Process Customer Personal Data for the Purposes, including, without limitation, Customer's sharing and/or receiving of Customer Personal Data with third-parties via the Services.

(b) In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which Customer 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 (including such as particularly for use by Customer for marketing purposes); (iii) ensuring Customer has the right to transfer, or provide access to, the Personal Data to Altinity for Processing in accordance with the terms of the Agreement (including this DPA); and (iv) ensuring that Customer instructions to Altinity regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws. Customer will inform Altinity without undue delay if it is not able to comply with its responsibilities under this Section 3.4 or applicable Data Protection Laws.

3.5 **Details of Data Processing.**

(a) Subject Matter: The subject matter of the Processing under this DPA is the Customer Personal Data.

(b) Frequency and Duration: Notwithstanding expiration or termination of the Agreement, Altinity will Process the Customer Personal Data continuously until deletion of all Customer Personal Data as described in this DPA.

(c) Purpose: Altinity shall Process the Customer Personal Data for the Purposes, as described in this DPA.

(d) Nature of the Processing: Altinity will perform Processing as needed for the Purposes, and to comply with Customer's Processing instructions as provided in accordance with the Agreement and this DPA.

(e) Retention Period. The period for which Customer Personal Data will be retained and the criteria used to determine that period shall be determined by Customer during the term of the Agreement via its use and configuration of the Service. Upon termination or expiration of the Agreement, Customer may retrieve or delete all Customer Personal Data as set forth in the Agreement. Any Customer Personal Data not deleted by Customer shall be deleted by Altinity promptly upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement.

(f) Categories of Data Subjects: The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);

(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors; and/or

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons).

(g) Categories of Personal Data: The categories of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, title, contact details);

(ii) Financial information (credit records, account details, payment information);

(iii) Employment details (employer, job title, geographic location, area of responsibility); and/or

(iv) IT information (IP addresses, usage data, cookies data, location data).

(h) Special Categories of Personal Data: The parties do not anticipate the transfer of "special categories of personal data" or similarly sensitive Personal Data (as described or defined in Data Protection Laws) in Customer Personal Data (e.g. Customer Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data Processed for the purposes of uniquely identifying a natural person, data concerning health and/or data concerning a natural person's sex life or sexual orientation).

4. Sub-processing.

Customer provides Altinity with a general authorization to engage Sub-Processors to Process Personal Data on Customer's behalf. Altinity has currently appointed, as Sub-Processors, the third parties listed in Annex A to this DPA. Altinity will notify Customer if it adds or removes Sub-Processors to Annex A prior to any such changes, if Customer opts-in to receive such email notifications by completing the form attached as Annex A-1. Where Altinity engages Sub-Processors, Altinity 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 (including, where appropriate, the SCCs), to the extent applicable to the nature of the services provided by such Sub-Processors. Altinity will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Altinity to breach any of its obligations under this DPA.

5. Security.

5.1 **Security Measures**. Altinity shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with the Security Measures described in Annex B (the "Security Measures"). Altinity may review and update its Security Measures from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

5.2 **Confidentiality of Processing**. Altinity shall ensure that any person who is authorized by Altinity to Process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3 **No Assessment of Customer Personal Data by Altinity**. Altinity shall have no obligation to assess the contents or accuracy of Customer Personal Data, or to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for reviewing the information made available by Altinity relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

6. Customer Audit Rights.

Altinity will make all information reasonably necessary to demonstrate compliance with this DPA available to Customer and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it will exercise its audit rights under this DPA by instructing Altinity to comply with the audit measures described in this Section 6. Customer acknowledges that the Service is hosted by Altinity's data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that Altinity's systems are regularly tested by independent third party penetration testing firms. Upon request, Altinity will supply (on a confidential basis) a summary copy of its penetration testing report(s) to Customer so that it can verify Altinity's compliance with this DPA. Further, at Customer's written request, Altinity will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer necessary to confirm Altinity's compliance with this DPA, provided that Customer will not exercise this right more than once per calendar year.

7. Data Transfers

7.1 **Hosting and Processing Locations.** Customer acknowledges and agrees that Altinity may access and Process Personal Data on a global basis as necessary to provide the Service in accordance with the Agreement, and in particular that Personal Data will be transferred to and Processed by Altinity, Inc. in the United States and to other jurisdictions where Altinity, its Affiliates and Sub-Processors have operations. Altinity will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

7.2 **Transfer Mechanisms.** For any transfers by Customer of Customer Personal Data from the European Economic Area and/or its member states, United Kingdom and/or Switzerland (collectively, "**Restricted Countries**") to Altinity in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the Data Protection Laws of the Restricted Countries) (collectively, "**Third Country**"), such transfers shall be governed by a valid mechanism for the lawful transfer of Customer Personal Data recognized under applicable Data Protection Laws, such as those directly below in 7.2.1. For clarity, for transfers from the United Kingdom and Switzerland, references in the SCCs shall be interpreted to include applicable terminology for those jurisdictions (e.g., "Member State" shall be interpreted to mean "United Kingdom" for transfers from the United Kingdom).

7.2.1 **SCCs**. Each party agrees to abide by, and transfer Customer Personal Data from the Restricted Countries in compliance with, the SCCs, which are incorporated into this DPA by reference. Each party is deemed to have executed the SCCs by entering into this DPA.

(a) The following subsections shall apply to the SCCs, including the election of specific terms and/or optional clauses as described in more detail in (i)-(x) below, and any optional clauses not expressly selected are not included:

(i) The Module 2 terms apply to the extent Customer is a Data Controller and the Module 3 terms apply to the extent Customer is a Data Processor of the Customer Personal Data;

(ii) The optional Clause 7 in Section I of the SCCs is incorporated, and Authorized Affiliates may accede to this DPA and the SCCs under the same terms and conditions as Customer, subject to Section 3.3 of this DPA via mutual agreement of the Parties;

(iii) For purposes of Clause 9 of the SCCs, Option 2 ("General written authorization") is selected and the process and time period for the addition or replacement of Sub-processors shall be as described in Section 4 (Sub-processing) of this DPA;

(iv) For purposes of Clause 13 and Annex 1.C of the SCCs, Customer shall maintain accurate records of the applicable Member State(s) and competent supervisory authority, which shall be made available to Altinity on request;

(v) For purposes of Clause 14(c), Customer may subscribe to the Sub-processor Site to receive notifications regarding updates to Altinity's overview of relevant laws and practices of Third Countries;

(vi) For purposes of Annex 1.A, the "data importer" shall be Altinity and the "data exporter" shall be Customer and any Authorized Affiliates that have acceded to the SCCs pursuant to this DPA;

(vii) For purposes of Annex 1.B, the description of the transfer is as described in Section 3.5 (Details of Data Processing) of this DPA;

(viii) For purposes of Annex 2, the technical and organization measures are as follows: (i) Those measures implemented by Altinity shall be as described in Section 5.1 (Security Measures) of this DPA; and (ii) Those measures that can be selected or configured by Customer, including appropriate controls for "special categories of data", shall be as further described in Altinity's Documentation; and

(ix) The Sub-processors for Annex III shall be as described in Section 4 (Authorized Sub-processors) of this DPA.

(b) **BCRS.** Notwithstanding the foregoing, if Altinity adopts Binding Corporate Rules (BCRs) for Processors that cover the transfer of Customer Personal Data to a Third Country, Altinity shall give Customer notice of such adoption and provide Customer with access to the BCRs, which shall govern the transfer of Customer Personal Data, effective from the date of such notice.

8. Security Incident Response.

8.1 **Security Incident Reporting.** If Altinity becomes aware of a Security Incident, Altinity shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after becoming aware. Altinity's notification shall be sent to the email registered by Customer within the Service for such purposes, and where no such email is registered, Customer acknowledges that the means of notification shall be at Altinity's reasonable discretion and Altinity's ability to timely notify shall be negatively impacted. Altinity shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

8.2 **Security Incident Communications.** Altinity shall provide Customer timely information about the Security Incident, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Altinity to mitigate or contain the Security Incident, the status of Altinity's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Altinity personnel do not have visibility to the content of Customer Personal Data, it will be unlikely that Altinity can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, number or categories of affected Data Subjects. Communications by or on behalf of Altinity with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Altinity of any fault or liability with respect to the Security Incident.

9. Cooperation.

9.1 **Data Subject Requests.** Altinity shall promptly notify Customer if Altinity receives a request from a Data Subject that identifies Customer Personal Data or otherwise identifies Customer, including a Data Subject's request to exercise its rights under applicable Data Protection Laws (each a "**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to Data Subject Requests and Customer will be responsible for responding to any such Data Subject Request. To the extent Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, Altinity shall (upon Customer's written request and taking into account the nature of the Processing, provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

9.2 **Data Protection Impact Assessments.** Altinity shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data

protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

9.3 **Government, Law Enforcement, and/or Third Party Inquiries.** If Altinity receives a demand to retain, disclose, or otherwise Process Customer Personal Data for any third party, including, but not limited to law enforcement or a government authority ("**Third-Party Demand**"), then Altinity shall attempt to redirect the Third-Party Demand to Customer. Customer agrees that Altinity can provide information to such third party as reasonably necessary to redirect the Third-Party Demand. If Altinity cannot redirect the Third-Party Demand to Customer, then Altinity shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy. This section does not diminish Altinity's obligations under the SCCs with respect to access by public authorities.

10. Relationship with the Agreement.

10.1 The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, annex, exhibit or standard contractual clauses that Altinity and Customer may have previously entered into in connection with the Services. Altinity may update this DPA from time to time, with such updated version posted to www.altinity.com/legal, or a successor website designated by Altinity; provided, however, that no such update shall materially diminish the privacy or security of Customer Personal Data.

10.2 Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Customer Personal Data comprised of patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state health care laws, rules or regulations ("**HIPAA Data**"), if there is any conflict between this DPA and a business associate agreement between Customer and Altinity ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data.

10.3 Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA, the SCCs, and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by one party (the "**Incurring Party**") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

10.4 In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the SCCs).

10.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

11. Parties to this DPA

11.1 **Permitted Affiliates.** By signing or otherwise agreeing to be bound by the the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of Customer's Authorized Affiliates, thereby establishing a separate DPA between Altinity and each such Authorized Affiliates subject to the Agreement and the 'General Provisions' and 'Parties to this DPA' sections of this DPA. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the purposes of this DPA only, and except where indicated otherwise, the terms "Customer" will include Customer and such Authorized Affiliates.

11.2 **Authorization**. The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Authorized Affiliates.

11.3 **Remedies**. Except where applicable Data Protection Laws require an Authorized Affiliate to exercise a right or seek any remedy under this DPA against Altinity directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Authorized Affiliates 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 such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with Altinity under the DPA and will be entitled to make and receive any communication related to this DPA on behalf of its Authorized Affiliates.

11.4 **Other Rights.** The parties agree that Customer will, when reviewing Altinity's compliance with this DPA pursuant to the Section 6 (Customer Audit Rights), take all reasonable measures to limit any impact on Altinity and its 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 Authorized Affiliates in one single audit.

In Witness Thereof, *the Parties have executed this Data Processing Addendum:*

CUSTOMER:	**ALTINITY:**
Company: _____	**Altinity, Inc.**
Address: _____	2001 Addison St., Suite 300,
_____	Berkeley, CA 94704, USA
_____	
Date: _____	Date: _____
Signature: _____	Signature: _____
Name: _____	Name: Mindaugas Zukas
Title: _____	Title: COO
Telephone: _____	Telephone: 628-400-4455
Email Address: _____	Email Address: info@altinity.com

Annex A
List of Sub-processors

Sub-Processor	Purpose	Location
Amazon Web Services, Inc.	Hosting & Infrastructure for management plane (Altinity Cluster Manager)	United States
Amazon Web Services, Inc	Hosting & Infrastructure of data plane used for Processing (Customer data warehouses)	Determined by location of Amazon data center selected by user.
Auth0, Inc	Authentication for access to management plane	United States
Google, Inc	Email to users as well as authentication to management plane. Hosting & Infrastructure of data plane used for Processing (Customer data warehouses)	United States Determined by location of Google data center selected by user.

Annex A-1

Request for notification of changes to List of Sub-processors

Annex B

Security Measures

This Annex forms part of the DPA.

Altinity currently observe the Security Measures described in this Annex B. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Master Terms.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems hosted by infrastructure provider(s) and accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

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

Data isolation: Customer data warehouses (data plane) are located in isolated environments for each Customer with dedicated storage, compute, and network resources.

ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

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

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

b) Transmission Control

In-transit: We apply HTTPS encryption (also referred to as TLS) available on all interfaces and for free on every customer site hosted on the Altinity products. Our HTTPS implementation uses industry standard encryption protocols and valid certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We provide the option for users to select at rest encryption for all data warehouse data. Users must select this option at cluster launch time.

c) Input Control
Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain 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 personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to Customer will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is replicated across availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 2 replicas. All databases are backed up and maintained using at least industry standard methods.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.