OPUS
Data Processing Agreement

1. Background

1.1. This Opus Data Processing Agreement and its Annexes ("**DPA**") is incorporated into and forms part of the Opus Subscriber Agreement, Opus Expert Cloud Terms of Use, or Opus Partner Marketplace Terms of Use between you and us (the "**Agreement**"). This DPA reflects the parties' agreement with respect to the Processing of Customer Personal Data by us as a Processor on your behalf.

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

1.3. The Processor-to-Controller terms apply solely to the extent that AppliedAI is a Processor of Customer Personal Data in connection with the Subscription Services.

1.4. We update these terms from time to time. We will let you know when we do through the Opus platform (the"**Platform**") or via email.

1.5. The term of this DPA will follow the term of the Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

2. Definitions

2.1. "**California Personal Information**" means Customer Personal Data that is subject to the protection of the CCPA.

2.2. "**CCPA**" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 or "**CPRA**").

2.3. "**Consumer**," "**Business**," "**Sell**," "**Service Provider**," and "**Share**" will have the meanings given to them in the CCPA.

2.4. "**Controller**" means 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.

2.5. "**Customer Personal Data**" means Personal Data contained within the data you upload to the Platform that AppliedAI Processes as a Processor on behalf of you.

2.6. "**Customer Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored, or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the services we provide to you. "Customer Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise

the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

2.7. "**Data Privacy Framework**" means the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded, or replaced.

2.8. "**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework; as may be amended, superseded, or replaced.

2.9. "**Data Protection Laws**" means all applicable worldwide legislation relating to data protection and privacy which applies to the Processing of Personal Data under the Agreement, including without limitation European Data Protection Laws, the CCPA, and other applicable U.S. federal and state privacy laws, and the data protection and privacy laws of Australia, Canada, Singapore, India, and Japan, in each case as amended, repealed, consolidated, or replaced from time to time.

2.10. "**Data Subject**" means the individual to whom Personal Data relates.

2.11. "**Europe**" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

2.12. "**European Data**" means Customer Personal Data that is subject to the protection of European Data Protection Laws.

2.13. "**European Data Protection Laws**" means data protection laws applicable in Europe, including: (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**"); (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (iv) Swiss Federal Data Protection Act and its Ordinance ("**Swiss DPA**"); in each case, as may be amended, superseded, or replaced.

2.14. "**Instruction**s" means the written, documented instructions issued by you to AppliedAI, and directing AppliedAI to perform a specific or general action with regard to Customer Personal Data (including, but not limited to, depersonalizing, blocking, deletion, and making available).

2.15. "**Personal Data**" means any information relating to an identified or identifiable individual where such information is protected similarly as personal data, personal information, or personally identifiable information under Data Protection Laws.

2.16. "**Processing**" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "**Process**," "**Processes**," and "**Processed**" will be construed accordingly.

2.17. "**Processor**" means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

2.18. "**Restricted Transfer**" means transfer of Personal Data originating from Europe to a country that does not provide an adequate level of protection within the meaning of applicable European Data Protection Laws.

2.19. "**Standard Contractual Clauses**" means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 currently found at https://eur-lex.europa.eu/eli/dec_impl/2021/914, as may be amended, superseded, or replaced.

2.20. "**Sub-Processor**" means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the Processing of Customer Personal Data under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any AppliedAI employee or consultant.

2.21. "**UK Addendum**" means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended, superseded, or replaced.

3. Customer responsibilities

3.1. Compliance with Laws. Within the scope of the Agreement and your use of the services, you will be responsible for complying with all requirements that apply to you under Data Protection Laws with respect to your Processing of Personal Data. In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Personal Data and the means by which you acquired such data; (ii) complying with all necessary transparency and lawfulness requirements under Data Protection Laws for the collection and use of Customer Personal Data, including providing adequate notices, obtaining any necessary consents and authorizations, and honoring opt-out preferences (particularly for use by you for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Customer Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); and (iv) complying with all laws applicable to any emails or other content created, sent, or managed through our services (including those relating to obtaining consents to send emails, the content of emails, and email deployment practices).

You will inform us without undue delay if you are not able to comply with your responsibilities under this 'Compliance with Laws' section or Data Protection Laws.

3.2. Customer Instructions. You are responsible for ensuring that your Instructions to us regarding the Processing of Customer Personal Data comply with applicable laws, including Data Protection Laws. The parties agree that the Agreement (including this DPA), together with your use of the services in accordance with the Agreement, constitute your complete Instructions to us in relation to our Processing of Customer Personal Data, so long as you may provide additional instructions during the Term that are consistent with the Agreement and the nature and lawful use of the services.

3.3. Security. You are responsible for independently determining whether the data security provided for in the services adequately meets your obligations under Data Protection Laws. You are also responsible for your secure use of the services, including protecting the security of Personal Data in transit to and from the services (including to securely backup or encrypt such data).

4. AppliedAI obligations as processor

4.1. Compliance with Instructions. We will only Process Customer Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

4.2. Conflict of Laws. If we become aware that we cannot Process Customer Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable services until such time as you issue new lawful Instructions with regard to the Processing.

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

4.4. Confidentiality. We will ensure that any personnel whom we authorize to Process Customer Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Customer Personal Data.

4.5. Customer Personal Data Breaches. We will notify you without undue delay after we become aware of any Customer Personal Data Breach and will provide timely information

relating to the Customer Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Customer Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

4.6. Deletion or Return of Customer Personal Data. We will delete or return all Customer Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of the Agreement. This term will apply except where we are required by applicable law to retain some or all of the Customer Personal Data, or where we have archived Customer Personal Data on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with our deletion practices.

5. Data subject requests

5.1. The Platform provides you with a number of controls that you can use to retrieve, correct, delete, or restrict Customer Personal Data, which you can use to assist you in connection with your obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under Data Protection Laws ("**Data Subject Requests**").

5.2. To the extent that you are unable to independently address a Data Subject Request through the Platform, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Customer Personal Data under the Agreement. You will reimburse us for the commercially reasonable costs arising from this assistance, and we will notify you of these costs in advance.

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

6. Sub-processors

6.1. You agree we may engage Sub-Processors to Process Customer Personal Data on your behalf, and we do so in three ways. First, we may engage Sub-Processors to assist us with hosting and infrastructure. Second, we may engage with Sub-Processors to support product features and integrations. Third, we may engage with third parties as Sub-Processors for service and support.

6.2. Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Customer Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. We 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 us to breach any of its obligations under this DPA.

7. Data transfers

7.1. You acknowledge and agree that we may access and Process Customer Personal Data on a global basis as necessary to provide the Platform services in accordance with the Agreement, and in particular that Customer Personal Data may be transferred to and Processed by AppliedAI in the United Arab Emirates and to other jurisdictions where Sub-Processors have operations. Wherever Customer Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

8. Demonstration of compliance

8.1. We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA, where required by applicable law. You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section.

8.2. Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year unless you have reasonable grounds to suspect noncompliance with the DPA.

9. Additional provisions for European Data

9.1. Scope. This 'Additional Provisions for European Data' section will apply only with respect to European Data that AppliedAI Processes on your behalf under the Agreement.

9.2. Role of Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are acting either as the Controller, or as a Processor on behalf of another Controller, and we are the Processor under the Agreement.

9.3. Instructions. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.

9.4. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities (for example, the French Data Protection Agency (CNIL), the Berlin Data Protection Authority (BlnBDI) and the UK Information Commissioner's Office

(ICO)) or other competent data privacy authorities to the extent required by European Data Protection Laws.

9.5. Data Transfers. We will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Customer Personal Data (within the meaning of applicable European Data Protection Laws), unless we first take all such measures as are necessary to ensure the transfer is in compliance 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 Customer Personal Data, including the Data Privacy Framework; (ii) to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws; or (iii) to a recipient that has executed the Standard Contractual Clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

10. Additional provisions for California Personal Information

10.1. Scope. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information that we Process on your behalf under the Agreement.

10.2. Role of Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.

10.3. Responsibilities. We certify that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Platform services under the Agreement (the "**Business Purpose**") or as otherwise permitted by the CCPA. Further, we certify that we will not (i) Sell or Share California Personal Information; (ii) Process California Personal Information outside the direct business relationship between the parties, unless required by applicable law; or (iii) combine California Personal Information included in Customer Data with Personal Data that we collect or receive from another source (other than information we receive from another source in connection with our obligations as a Service Provider under the Agreement).

10.4. Compliance. We will (i) comply with the obligations applicable to us as a Service Provider under the CCPA; (ii) provide the same level of protection for California Personal Information as is required by the CCPA; and (iii) notify you if we make a determination that we can no longer meet our obligations as a Service Provider under the CCPA.

10.5. CCPA Audits. You will have the right to take reasonable and appropriate steps to help ensure that we use California Personal Information in a manner consistent with your obligations under the CCPA. Upon notice, you will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of California Personal Information.

10.6. Not a Sale. The parties acknowledge and agree that the disclosure of California Personal Information by you to us does not form part of any monetary or other valuable consideration exchanged between the parties.

11. Transfer mechanisms

Where the transfer of Customer Personal Data or Controller Personal Data between the parties involves a Restricted Transfer and European Data Protection Laws require putting in place appropriate safeguards, the Parties will comply with the following:

11.1. Data Privacy Framework. AppliedAI participates in and certifies compliance with the Data Privacy Framework. Where and to the extent the Data Privacy Framework applies, we will use the Data Privacy Framework to lawfully receive Customer Personal Data and Controller Personal Data in the United States and will provide at least the same level of protection to such data as is required by the Data Privacy Framework Principles. We will inform you if we are unable to comply with this requirement.

11.2. Standard Contractual Clauses. If European Data Protection Laws require that appropriate safeguards are put in place (for example, if the Data Privacy Framework does not cover the transfer and/or the Data Privacy Framework is invalidated), the Standard Contractual Clauses will be incorporated by reference and form part of the Agreement as follows:

11.2.1. In relation to Customer Personal Data that we Process as a Processor (i) the Module Two terms apply to the extent you are a Controller and the Module Three terms apply to the extent you are a Processor of Customer Personal Data; (ii) in Clause 7, the optional docking clause applies; (iii) in Clause 11, the optional language is deleted; (iv) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be the Republic of Ireland (without reference to conflicts of law principles); (v) the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in the Annexes of this DPA; and (vi) the supervisory authority that will act as competent supervisory authority will be determined in accordance with GDPR.

11.2.2. In relation to Customer Personal Data that is subject to the UK GDPR, the Standard Contractual Clauses will apply in accordance with sub-section (A) and the following modifications (i) the Standard Contractual Clauses will be modified and interpreted in accordance with 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 deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting "neither party"; and (iii) any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

11.2.3. In relation to Customer Personal Data and Controller Personal Data that is subject to the Swiss DPA, the Standard Contractual Clauses will apply in accordance with

sub-section (A) and the following 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."

11.2.4. In relation to Customer Personal Data that we Process as a Processor, you agree that by complying with our obligations under the 'Sub-Processors' section of this DPA, we fulfill our obligations under Section 9 of the Standard Contractual Clauses. For the purposes of Clause 9(c) of the Standard Contractual Clauses, you acknowledge that we may be restricted from disclosing Sub-Processor agreements but we will use reasonable efforts to require any Sub-Processor we appoint to permit it to disclose the Sub-Processor agreement to you and will provide (on a confidential basis) all information we reasonably can. You also acknowledge and agree that you will exercise your audit rights under Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the measures described in the 'Demonstration of Compliance' section of this DPA.

11.3. Alternative transfer mechanism. In the event that we are required to adopt an alternative transfer mechanism under European Data Protection Laws, in addition to or other than the mechanisms described 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 complies with European Data Protection Laws), and you agree to execute such other documents or take such action as may be reasonably necessary to give legal effect such alternative transfer mechanism.

12. General provisions

12.1. Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to the ‘Compliance with Instructions’ or ‘Security’ sections of this DPA, we reserve the right to make any updates and changes to this DPA.

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

12.3. 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 data processing agreements 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 such section to the liability of a party means aggregate liability of that party and all of its affiliates under the Agreement (including this DPA).

12.4. Governing Law. This DPA will be governed by and construed in accordance with the laws of the Abu Dhabi Global Market, unless required otherwise by Data Protection Laws.

13. Parties to this DPA

13.1. Authorization. The legal entity agreeing to this DPA 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 affiliates.

13.2. Remedies. The parties agree that (i) solely the entity that is the contracting party to the Agreement will exercise any right or seek any remedy any affiliate may have under this DPA on behalf of its Affiliates, and (ii) the entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each affiliate individually but in a combined manner for itself and all of its affiliate together. The entity that is the contracting entity is responsible for coordinating all Instructions, authorizations and communications with us under the DPA and will be entitled to make and receive any communications related to this DPA on behalf of its affiliate.

13.3. Other Rights. The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on us and our affiliates by combining several audit requests carried out on behalf of the entity that is the contracting party to the Agreement and all of its affiliates in one single audit.

ANNEX 1 - DETAILS OF PROCESSING

A. LIST OF PARTIES

Data exporter:

Name: You (on behalf of yourself and affiliates)

Address: Your address, as set out in your Account.

Contact person's name, position and contact details: Your contact details, as set out in the your Account

Activities relevant to the data transferred under these Clauses: Processing of Customer Personal Data in connection with your use of the Platform Services under the terms of the Agreement.

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: Applied AI Corporation Limited

Address: Level 5, C11 Building 2, Khaleej Street, Khalifa Park, Al Muntazah Zone 1, Abu Dhabi

Contact person's name, position and contact details: Saurav Das, Legal Counsel, legal@aaico.com

Activities relevant to the data transferred under these Clauses: Processing of Customer Personal Data in connection with your use of the Platform services under the terms of the Agreement.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is Transferred

You may submit Customer Personal Data in the course of using the Platform services, the extent of which is determined and controlled by you in your sole discretion.

Categories of Personal Data Transferred

You may submit Personal Data to the Platform services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

1. Contact Information.

2. Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Platform services.

Sensitive Data Transferred and Applied Restrictions or Safeguards

The processing of Sensitive Data is subject to the scope limitations, restrictions, and safeguards mutually agreed upon by the parties, as reflected in the Agreement.

Frequency of the Transfer:

Continuous

Nature of the Processing

Customer Personal Data will be Processed in accordance with 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 Platform services provided to you; and/or

2. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

Purpose of the Transfer and Further Processing

We will Process Customer Personal Data as necessary to provide the Platform services pursuant to the Agreement and as further instructed by you in your use of the Platform services.

Period for which Personal Data will be retained

Subject to the 'Deletion or Return of Customer Personal Data' section of this DPA, we will Process Customer Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

ANNEX 2: SECURITY MEASURES

1. ACCESS CONTROL

1.1. Preventing Unauthorized Product Access. Outsourced processing: We host our Platform with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Platform 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.

1.1.1. Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems. The infrastructure providers' physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

1.1.2. 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 Customer Personal Data in their account.

1.1.3. Authorization: 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 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.

1.1.4. Application Programming Interface (API) access: Public product APIs may be accessed using Oauth authorization or private app tokens.

1.2. Preventing Unauthorized Product Use. We implement industry standard access controls and detection capabilities for the internal networks that support its products.

1.2.1. 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.

1.2.2. 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.

1.2.3. Static code analysis: Code stored in our source code repositories is checked for best practices and identifiable software flaws using automated tooling.

1.2.4. Endpoint Hardening: Endpoints are hardened in accordance with industry standard practice. Workstations are protected using anti-malware and endpoint detection & response tools, receiving regular definition and signature updates.

1.3. Limitations of Privilege and Authorization Requirements. Privileged Access Management: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or "**JITA**") controls. Non-personal accounts used for system access are stored in a secure vault with additional controls governing privilege elevation and account check out processes.

1.3.1. 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, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through JITA requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months.

2. TRANSMISSION CONTROL

2.1. In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces. Our HTTPS implementation uses industry standard algorithms and certificates.

2.2. At-rest: We store user passwords following policies that follow industry standard practices for security. We take a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted.

3. INCIDENT MANAGEMENT, LOGGING, AND MONITORING

3.1. Incident Response Plan: We maintain an Incident Response Plan, playbooks, and other necessary processes and procedures to fulfill the standards and obligations reflected therein.

3.2. Detection: We 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 appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

3.3. 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 you will be in accordance with the terms of the Agreement.

4. AVAILABILITY CONTROL

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

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

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

4.4. Disaster Recovery Plans: We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes.

4.5. 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.

5. VULNERABILITY MANAGEMENT PROGRAM

5.1. Vulnerability Remediation Schedule: We maintain a vulnerability remediation schedule aligned with industry standards. We take a risk-based approach to determining a vulnerability's applicability, likelihood, and impact in our environment.

5.2. Vulnerability scanning: We perform daily vulnerability scanning on our products using technology and detection standards aligned with industry standards.

5.3. Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for penetration testing of both the Platform and internal corporate network infrastructure at least annually. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems.

6. PERSONNEL MANAGEMENT

6.1. We staff qualified personnel to develop, maintain, and enhance our security program. We train all employees on security policy, processes, and standards relevant to their role and in accordance with industry practice.

6.2. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.