Private Preview Agreement for Apollo Dedicated

Last updated: September 27, 2023

This Private Preview Agreement for Apollo Dedicated ("PPA") is between Apollo Graph, Inc. ("Apollo") and the Customer identified in an Order ("Customer" or "you"). Further, this PPA (i) will govern the use and provision of Cloud Services purchased by Customer; (ii) does not have to be signed to be binding; and (iii) is effective as of the effective date of an Order signed by both Customer and Apollo ("Effective Date").

You acknowledge that Apollo may make changes to this PPA from time to time (with or without notice) and your continued use of the Cloud Services will constitute consent to such changes. If you do not agree to the revised PPA, you must stop using the Cloud Services.

For clarity, this PPA ***only*** pertains to the Cloud Services described below and does not pertain to any of Apollo's (i) self-service offerings, which are separately governed by the Self-Service Subscription Agreement, or (ii) enterprise offerings, which are separately governed by either the Enterprise Master Services Agreement or a separate written agreement.

1. **Definitions**

"Affiliate" of a party means an entity that controls, is actually or in effect controlled by, or is under common control with such party. For purposes of this PPA, "control" means owning or otherwise controlling more than 50% of the voting interests of an entity.

"Agreement" means this PPA together with any applicable Order(s).

"Cloud Environment" means a cloud or other computer or storage infrastructure controlled by a party.

"Cloud Services" means Apollo's proprietary hosted or cloud-based solution(s) currently referred to as "Apollo Dedicated" (as may be rebranded by Apollo at any time), inclusive of any applicable and included SaaS, open-source software, source-available software, products, processes, algorithms, user interfaces, know-how, techniques, designs and other tangible or intangible technical material or information.

"Confidential Information" means any business or technical or non-technical information disclosed by or on behalf of either party or their Affiliates to the other that is designated as confidential at the time of disclosure or that, under the circumstances, a person exercising reasonable business judgment would understand to be confidential or proprietary. Without limiting the foregoing, all non-public elements of the Cloud Services are Apollo's Confidential Information, Customer Data is Customer's Confidential Information, and any information that either party conveys to the other party concerning data security measures, incidents, or findings constitute Confidential Information of both parties. Confidential Information will not include information that the receiving party can demonstrate (a) is or becomes publicly known through no fault of the receiving party, (b) is, when it is supplied, already known to whoever it is disclosed to in circumstances in which they are not prevented from disclosing it to others, (c) is independently obtained by whoever it is disclosed to in circumstances in which they are not prevented from disclosing it to others or (d) was independently developed by the receiving party without use of or reference to the Confidential Information.

"Customer Data" means any data, information, or material that Customer or Users disclose or submit to Apollo in the course of using the Cloud Services.

"Data Protection Laws" means all applicable local, state, federal and international laws, regulations and conventions, including those related to data privacy and data transfer, international communications and the exportation of technical or personal data.

"Documentation" means the documentation related to the Cloud Services, as made available by Apollo.

"Order" means the document signed by an authorized representative of each party that references this PPA and identifies the specific Cloud Services to be made available and the fees to be paid.

"Subscription Term" means Customer's permitted subscription period for the Cloud Services, as set forth in the applicable Order.

"Use Limits" means, as applicable, any numerical limits or restrictions on the units of measure referenced in an Order or as set forth in the Cloud Services interface.

"User(s)" means Customer's employees, representatives, consultants, contractors or agents who are authorized by Customer to access the Cloud Services on Customer's behalf.

"Utilization Data" means data and telemetry relating to Customer's use of the Cloud Services, but expressly excludes any Customer Data or other identifiable data.

2. **Use of Cloud Services**

2.1. **Access and Use.** Subject to the terms and conditions of this PPA and during the applicable Subscription Term, Customer and its Users may access and use the Cloud Services for the internal business purposes of Customer and/or its Affiliates, as applicable, in accordance with the applicable Order and the Documentation. The foregoing rights granted to Customer are non-exclusive, non-sublicensable, and non-transferable.

2.2. **Apollo Responsibilities.**

2.2.1. **Services.** Apollo is responsible for (a) the operation of the Apollo Cloud Environment; and (b) the Apollo software used to operate the Cloud Services.

2.2.2. **Security Measures.** Apollo will maintain security protections for the Cloud Services as described in the Security Policy attached hereto as Exhibit B ("Security Policy"), including any relevant certifications. Any security updates will not lessen these measures. With respect to Customer Data properly submitted to the Cloud Products for processing by Apollo, Apollo will maintain commercially reasonable administrative, physical, and technical safeguards designed to prevent unauthorized access to or use of Customer Data, in accordance with the Security Policy.

2.2.3. **Support and Service Level Credits.** Apollo will provide you with the level or type of support specified in an Order. If support is not specified in an Order, Customer's support shall be limited to public Documentation and non-enterprise support. For clarity, (i) the sole service level agreements or service level credits to which Customer is entitled hereunder are set forth as Exhibit A attached hereto; and (ii) any other service level agreements or service level credits applicable to other Apollo offerings are expressly excluded from this PPA.

2.3. **Customer Responsibilities.**

2.3.1. **General Responsibilities.** Customer is responsible for: (a) its Users' compliance with this Agreement, inclusive of not sharing unique credentials; (b) securing Customer's Cloud Environment and systems; (c) backing up Customer Data; and (d) determining the Customer Data that Customer chooses to process using the Cloud Services.

2.3.2. **Data Compliance Obligations.** Customer and its Users must comply at all times with the terms and conditions of this PPA and Data Protection Laws. Customer represents and warrants that: (i) Customer has obtained all necessary rights, releases, and permissions to submit Customer Data to the Cloud Services and to grant the rights granted to Apollo hereunder and (ii) Customer Data and its submission and use as authorized in the Agreement will not violate any (1) Data Protection Laws, or (2) third-party intellectual property, privacy, publicity or other rights.

2.3.3. **Restrictions.** Customer will not and will ensure its Affiliates and Users do not: (a) use the Cloud Services other than in accordance with this Agreement and the Documentation; (b) copy, modify, disassemble, decompile, reverse engineer, or attempt to view or discover the source code of the Cloud Services, in whole or in part, or permit or authorize a third party to do so, except to the extent such activities are expressly permitted by the Agreement or by law; (c) sell, resell, license, sublicense, distribute, rent, lease, or otherwise provide access to the Cloud Services to any third party except to the extent explicitly authorized in writing by Apollo; (d) use the Cloud Services to develop or offer a service made available to any third party that could reasonably be seen to serve as a substitute for such third party's possible purchase of any Apollo services or offerings; (e) attempt to interfere with, harm, or disrupt the Cloud Services, or use any means to bypass usage limitations; (f) abuse or violate the security or integrity of any system of any party, including, without limitation, by storing, transmitting or installing malicious code; (g) process, store, or transmit data or content in violation of any law or any third party rights; and/or (h) transfer or assign any of its respective rights hereunder.

2.3.4. **Third-Party Applications.** Customer may choose to use other third-party applications in connection with the Cloud Services. Customer's use of any third party applications is subject to a separate agreement between Customer and the third party provider. If Customer enables or uses third party applications with the Cloud Services, Apollo may allow the third-party providers to access or use Customer Data as required for the interoperation of third-party applications with the Cloud Services. This may include transmitting, transferring, modifying or deleting Customer Data, or storing Customer Data on systems belonging to the third-party providers or other third parties. Any third-party provider's use of Customer Data is subject to the applicable agreement between Customer and such third-party provider. Apollo is not responsible for any access to or use of Customer Data by third-party providers, or for the security or privacy practices of any third-party provider. Customer is solely responsible for its (or its Users') decision to permit any third-party provider to use Customer Data. It is Customer's responsibility to carefully review the agreement between Customer and the third-party provider. APOLLO DISCLAIMS ALL LIABILITY AND RESPONSIBILITY FOR ANY THIRD-PARTY APPLICATIONS (WHETHER SUPPORT, AVAILABILITY, SECURITY, OR OTHERWISE) OR FOR THE ACTS OR OMISSIONS OF ANY SUCH THIRD-PARTY PROVIDERS.

2.4. **Customer Data.**

2.4.1. **Content.** Customer agrees Customer Data will not include any data for which Customer does not have all rights, power and authority necessary for its processing as contemplated by the Agreement.

2.4.2. **Sensitive Data.** Customer agrees Customer Data will not include any protected health information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or any cardholder data as defined under PCI-DSS ("Cardholder Data") unless Customer has entered into an Order permitting the processing of PHI and/or Cardholder Data. Apollo will have no liability under the Agreement relating to PHI or Cardholder Data that is not processed in accordance with the terms of this Section notwithstanding anything in the Agreement or, as applicable, in HIPAA, PCI-DSS, or Data Protection Laws, or any other laws to the contrary.

2.5. **Data Protection.** Apollo will maintain commercially reasonable administrative, physical, and technical safeguards designed to prevent unauthorized access to or use of Customer Data.

3. **Intellectual Property**

3.1. **Apollo Ownership.** Apollo retains all rights, title, and interest in and to the Cloud Services, Feedback (as defined below), Utilization Data, and any derivative works, modifications, or improvements of any of the foregoing, and no ownership transfers to Customer.

3.2. **Customer Ownership.** Customer retains all rights, title, and interest in and to the Customer Data and no ownership transfers to Apollo.

3.3. **Utilization Data.** Apollo is expressly permitted to use Utilization Data to develop, improve, and support its products and services.

3.4. **Feedback.** If Customer chooses to offer suggestions or other feedback to Apollo pertaining to the Cloud Services ("Feedback"), Customer hereby grants Apollo a perpetual, irrevocable, non-exclusive, worldwide, fully-paid, sub-licensable, assignable license to use the Feedback to improve Apollo products and services, provided that such Feedback is used in a manner not attributable to Customer.

4. **Confidentiality**

4.1. **Use and Disclosure.** A receiving party will not use the disclosing party's Confidential Information except as permitted under the Agreement or to enforce its rights under the Agreement and will not disclose such Confidential Information to any third party except to those of its employees, Affiliates, and/or subcontractors who have a bona fide need to know such Confidential Information for the performance or enforcement of the Agreement and are bound by written confidentiality obligations at least as stringent as this Section 2. Both parties must protect this information using a reasonable standard. If legally mandated, a party can disclose the information, provided the other party is given notice to contest or limit the request. This supersedes previous non-disclosure agreements.

4.2. **Breach Consequences.** A breach of confidentiality can result in irreparable damage. In such cases, the affected party can seek injunctive relief alongside other legal remedies.

5. **Payment of Fees.**

5.1. **Fees and Invoices.** Customer agrees to pay all fees specified in the applicable Order. Except as otherwise specified in such Order(s): (a) all fees are payable in USD; (b) invoiced payments will be due within 30 days of the invoice date; (c) fees for all prepaid committed Cloud Services will be invoiced in full upon execution of the applicable Order; and (d) to the extent applicable, all excess Cloud Services usage will be invoiced monthly in arrears. All past due payments, except to the extent reasonably disputed, will accrue interest at the highest rate allowed under applicable laws but in no event more than one and one-half percent (1.5%) per month.

5.2. **Credit Card Payment Method.** If Customer pays via credit card, Customer will provide an authorized credit card for all fees set forth in the applicable Order (and for each subsequent renewal). By providing a credit card, Customer expressly authorizes Apollo to charge Customer, as set forth on the Order, on a monthly, annual, or pay-as-you-go basis, or as otherwise applicable for the Fees. Customer further acknowledges that Apollo uses a third-party company to facilitate such payments and expressly agrees that Apollo shall have no liability for Customer's credit card information.

5.3. **Use Limit Overages.** If the Customer exceeds the Use Limits as set forth in any applicable Order, then Customer will be invoiced monthly in arrears for the overage. For clarity, if Customer has a credit card on file (in accordance with Section 5.2 above), such credit card will be charged for such Use Limit overages.

5.4. **Taxes.** Customer is solely responsible for payment of any applicable sales, value added or use taxes, or similar government fees or taxes. To the extent that Customer enters into an Order via a marketplace, Customer agrees that should Customer fail to pay fees when due to or through the applicable marketplace, Apollo may seek payment directly from Customer.

6. Term and Termination

6.1. **Term of PPA.** This PPA will become effective on the Effective Date and will continue in full force and effect until terminated by either party as set forth herein. This PPA will automatically expire when all affiliated Orders issued hereunder are terminated or expired.

6.2. **Term of Order(s); Renewals.** An Order may specify the effective duration of the Cloud Services purchased under such Order. Except as otherwise stated in an Order, unless either party provides notice of non-renewal (email sufficing) prior to expiration of the current Subscription Term, an Order will automatically renew for another Subscription Term of a period equal to the initial Subscription Term. All renewals are subject to the applicable Cloud Services continuing to be offered and will be charged at the then-current rates.

6.3. **Termination for Cause.** The Agreement, including Customer's use of the Cloud Services and any Apollo Cloud Environment, may be terminated (i) by either party on thirty (30) days' prior written notice if the other party is in material breach of the Agreement and the breaching party fails to cure the breach prior to the end of the notice period; or (ii) by Apollo immediately following receipt of a notice that you are delinquent in the payment of undisputed fees. If the Agreement terminates pursuant to the prior sentence due to Apollo's material breach, Apollo will refund that portion of any prepayments related to Cloud Services not yet provided.

6.4. **Additional Apollo Termination Rights.** Apollo may terminate the Agreement at any time for convenience, without causing any breach or incurring any additional obligation, liability, or penalty, upon thirty (30) days' notice (email sufficing). If the Agreement terminates pursuant to this Section 6.4 (Additional Apollo Termination Rights), Apollo will refund that portion of any prepayments related to Cloud Services not yet provided.

6.5. **Suspension and Effects of Expiration/Termination.**

6.5.1. **Suspension.** Apollo can suspend all or any portions of Cloud Services at any time: (a) immediately without notice if Apollo reasonably suspects that Customer has violated its obligations under Section 2.3 (Customer Responsibilities), Section 2.4 (Customer Data), or accesses or uses the Cloud Services in a manner that may cause material harm or material risk of harm to Apollo or to any other party; (b) if Customer fails to pay undisputed Fees after receiving notice that you are delinquent in payment; or (c) if Customer intentionally or materially exceeds Use Limits.

6.5.2. **Effects of Expiration/Termination.** Upon any expiration or termination of the Agreement, Customer must cease using all Cloud Services and delete or return (at Apollo's request) all Apollo Confidential Information in Customer's possession. For clarity, Customer will not have access to Customer Data and Apollo will delete all Customer Data after expiration or termination of the Agreement unless legally prohibited. In no event will termination relieve Customer of its obligation to pay any fees payable to Apollo for the period prior to the effective date of termination. Except where an exclusive remedy may be specified in this PPA, the exercise by either party of any remedy, including termination, will be without prejudice to any other remedies it may have hereunder, by law or otherwise.

6.6. **Survival.** The following provisions will survive any termination or expiration of these Terms: Sections 2.3.3 (Restrictions), 8 (Indemnification), 6.1 (Third-Party Products), 9.4 (Payment), 11 (Taxes not included), 14 (Evaluations, trials, and betas) (disclaimers and use restrictions only), 15 (IP Rights in the Cloud Products and Feedback), 16 (Confidentiality), 17 (Term and Termination), 18.4 (Warranty Disclaimer), 19 (Limitations of Liability), 20 (IP Indemnification) (but solely with respect to claims arising from your use of Cloud Products during the Subscription Term), 22 (Dispute Resolution) and 26 (General Provisions).

7. **Disclaimer of Warranty.** THE CLOUD SERVICES ARE PROVIDED "AS IS" AND APOLLO MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND APOLLO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE OR ANY IMPLIED WARRANTIES ARISING OUT OF THE COURSE OF DEALING OR THE USAGE OF TRADE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. APOLLO DOES NOT WARRANT THAT THE CLOUD SERVICES ARE OR WILL BE ERROR-FREE.

8. **Indemnification.** Customer will defend, indemnify, and hold harmless Apollo (and Apollo's Affiliates, officers, directors, agents and employees) from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) resulting from any claim arising from or related to Customer's breach (or alleged breach) of Section 2.3.2 (Data Compliance Obligations) and/or Section 2.5 (Customer Data). This indemnification obligation is subject to Customer receiving (a) prompt written notice of such claim (but in any event notice in sufficient time for Customer to respond without prejudice); (b) the exclusive right to control and direct the investigation, defense or settlement of such claim and (c) all reasonable necessary cooperation by Apollo at Customer's expense.

9. **Limitation of Liability.** TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL APOLLO BE LIABLE FOR ANY DAMAGES, OF WHATEVER NATURE, AS A RESULT OF THIS AGREEMENT OR THE CLOUD SERVICES, INCLUDING BUT NOT LIMITED TO ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, EXEMPLARY, INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES OF ANY TYPE OR KIND (INCLUDING LOSS OF REVENUE, PROFITS, USE OR OTHER ECONOMIC ADVANTAGE) ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THIS AGREEMENT OR USE OF THE SERVICES, INCLUDING BUT NOT LIMITED TO THE USE OR INABILITY TO USE THE CLOUD SERVICES, ANY INTERRUPTION, INACCURACY, ERROR OR OMISSION, REGARDLESS OF CAUSE, EVEN IF APOLLO HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

10. **General/Notices.** This Agreement shall be governed by California law and controlling United States federal law, without regard to the choice or conflicts of law provisions of any jurisdiction, and any disputes, actions, claims or causes of action arising out of or in connection with this Agreement or the Cloud Services shall be subject to the exclusive jurisdiction of the state and federal courts located in San Francisco, California. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, then such provision(s) shall be construed, as nearly as possible, to reflect the intentions of the invalid or unenforceable provision(s), with all other provisions remaining in full force and effect. No joint venture, partnership, employment, or agency relationship exists between Customer and Apollo as a result of this Agreement or use of the Cloud Services. The failure of either party to enforce any right or provision in this Agreement shall not constitute a waiver of such right or provision unless acknowledged and agreed to by such party in writing. This Agreement, (including any other documents referenced therein), comprises the entire agreement between Customer and Apollo regarding the subject matter contained herein and supersedes all prior or contemporaneous negotiations, discussions or agreements, whether written or oral, between the parties regarding such subject matter. No terms or conditions stated in any customer purchase order, vendor onboarding process or web portal, or any other of your company's or organization's order documentation (excluding Orders) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void, notwithstanding any language to the contrary therein, whether signed before or after this Agreement. All notices from Customer to Apollo may be made by emailing legal@apollographql.com and Apollo may give notice by emailing Customer's contact(s) as specified in an applicable Order.

Exhibit A

Service Level Addendum

This Service Level Addendum ("SLA") solely applies to the Cloud Services referenced in the PPA and applicable Order(s), but does not apply to separate Apollo offerings made available with or connected to the Cloud Services (including any Apollo offerings hosted by Customer). Capitalized terms used but not defined in this SLA will have the meaning assigned to them in the PPA.

1. **Uptime Commitment**. During the Subscription Term, Apollo will make the Cloud Services available an average of at least 99.9% of the time ("Uptime Commitment"), measured on a monthly basis, excluding (a) scheduled downtime, or (b) any unavailability or downtime caused by any circumstance excluded under Section 3 below.
2. **Credits**. In the event that Apollo fails to meet the Uptime Commitment in a given month ("Service Level Failure"), then as Customer's sole and exclusive remedy, Customer shall receive the applicable credits set forth below ("Service Level Credits"), credited against Customer's renewal Fees for the renewal Subscription Term following the then-current Subscription Term, provided that Customer requests Service Level Credits within twenty-one (21) days of the calendar month in which the Service Level Failure occurred. For clarity, Service Level Credits may not be exchanged for, or converted to, monetary amounts.

Availability	Service Level Credit
Under 99.9%	10% of the Average Monthly Fee

For purposes of this SLA, the "Average Monthly Fee" means the average monthly Fees of the current Subscription Term purchased by Customer on the Order. For example, if Customer purchases a six month subscription of $30,000.00 USD, then the Average Monthly Fee is $5,000.00 U.S.D. For example, using the hypothetical Average Monthly Fee noted in this Section 2, if, during one month of the Subscription Term, the Service Level Failure is at 99.0%, then Customer's Service Level Credit equals 10% of $5,000 USD, or $500 USD.

3. **SLA Exclusions**. This SLA and the Uptime Commitment do not apply to any performance or availability issues: (a) due to factors outside Apollo's reasonable control (for example, a network or device failure external to Apollo's data centers); (b) that resulted from Customer's use of equipment, software, or services not provided by Apollo as part of the Cloud Services; (c) due to Customer's use of the Cloud Services in a manner inconsistent with the features and functionality of the Cloud Services or inconsistent with the Documentation; (e) caused by Customer's use of the Cloud Services after Apollo advised Customer to modify its use of the Cloud Services, if Customer did not modify its use as advised; (f) that resulted from Customer's attempts to exceed any applicable Use Limits; or (g) attributable to acts by persons gaining unauthorized access to the Cloud Service by means of Customer's passwords or equipment or otherwise resulting from Customer's failure to follow appropriate security practices.
4. **Additional Termination Right**. In addition to Service Level Credits, Customer may terminate the affected Order on written notice to Apollo if Apollo fails to meet the Uptime Commitment in any three (3) months in any rolling twelve (12) month period, in which case Customer shall receive a pro-rata refund of pre-paid Fees remaining for the then-current Subscription Term.

EXHIBIT B
SECURITY POLICY

This Apollo Graph, Inc. Information Security Policy ("**Security Policy"**) describes Apollo's security procedures and safeguards that Apollo uses in connection with the hosting and provision of the Cloud Services that processes Customer Data (as each term is defined in the Agreement). Apollo implements a comprehensive documented security program based on NIST 800-53 (or industry recognized successor framework), under which Apollo implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Cloud Services and Customer Data (the "**Security Program**"), including, but not limited to, as set forth below. Apollo regularly tests and evaluates its Security Program and may review and update its Security Program as well as this Security Policy, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

Apollo utilizes third party Hosting Partners as set forth in the Documentation (each, a "**Hosting Partner**") and provides the Cloud Services to Customer from a VPC/VNET hosted by the applicable Hosting Partner (the "**Cloud Environment**").

1. **Security Officer Role**

Apollo's vice president of engineering in charge of oversight and enforcement of the Security Program ("Security Officer"). The Security Officer is responsible for creating and enforcing the Security Policies herein; including the monitoring, vulnerability management, and incident detection and response initiatives; and tracking and reducing risk organization-wide.

2. **Operations Security**

2.1. Background Screens. All Apollo employees undergo pre-employment background checks consistent with SOC 2 Type II requirements and applicable law, where permitted in the jurisdiction in which the candidate and/or employee are located. Apollo may rescind an employee's offer letter if their background check is found to be falsified, erroneous, or misleading and will not assign personnel to any role in which such personnel has access to Customer Data unless a background check has been completed for that individual and no issues were found.

2.2. Security Awareness Training. Apollo employees and contractors with privileged access to Customer Data are provided training on the company's security policies and procedures annually. All Apollo personnel are required to acknowledge, electronically, that they have attended training and understand the security policy.

2.3. Security Coding Training. Apollo employees and contractors in developer roles are provided with SDLC / Secure Coding training annually. Software developers are trained in secure coding techniques, including how to avoid common coding vulnerabilities. All such personnel are required to acknowledge, electronically, that they have attended and understand SDLC training and OWASP Top Ten common coding vulnerabilities.

2.4. Acceptable Use Policy. Apollo maintains an internal Acceptable Use Policy that covers employee responsibilities and behavior for using Apollo's systems, including devices, email, internal tools, and social media. Apollo employees must acknowledge in writing that they've read and will abide by the Acceptable Use Policy.

2.5. Remote Work. Apollo employees who work remotely must follow these rules:

- All company-provided equipment and any equipment used to perform work must remain in the presence of the Apollo employee or be securely stored.
- VPN must be used for all connections with production infrastructure.
- All of Apollo's data encryption, protection standards and settings must be followed for company-provided equipment and any equipment used to perform work.
- The confidentiality, security and privacy of Apollo's customers must be preserved by taking steps to verify that no unauthorized individuals may view, overhear, or otherwise have access to Customer Data.
- To enforce the foregoing requirements, all Apollo employees are required to use screen protectors or be conscious of "shoulder surfing" when working in public places like a coffee shop or airport. Apollo employees are further required not to teleconference with customers in public areas.
- All remote work must be performed in a manner consistent with Apollo's security policies.

2.6. Disciplinary Action. Employees who violate either the Acceptable Use Policy or this Security Policy may face disciplinary consequences in proportion to their violation. Apollo management will determine how serious an employee's offense is and take the appropriate action: For minor violations, employees may only receive verbal reprimands. For more serious violations, employees may face severe disciplinary actions up to and including termination.

2.7. Employee Access**.** Apollo will revoke employee's access to physical locations, systems, and applications that contain or process Customer Data within one (1) business day of the cessation of such employee's need to access the system(s) or application(s).

3. **Apollo's Audits & Certifications**

3.1. The information security management system supporting the Cloud Services shall be assessed by one or more independent third-party auditors in accordance with the following audits and certifications ("**Third-Party Audits**"), on at least an annual basis: SOC 2 Type I

3.2. To the extent Apollo discontinues a Third-Party Audit, Apollo will adopt or maintain an equivalent, industry-recognized framework.

4. **Hosting Location of Customer Data**

4.1. The hosting location of Customer Data is in the United States.

5. **Encryption**

5.1. Apollo encrypts Customer Data at-rest using AES 256-bit (or better) encryption. Apollo leverages Transport Layer Security (TLS) 1.2 (or better) for Customer Data in-transit over untrusted networks.

5.2. Apollo's encryption key management conforms to NIST 800-53 and involves regular rotation of encryption keys. Hardware security modules are used to safeguard top-level encryption keys. Apollo logically separates encryption keys from Customer Data.

6. **System & Network Security**

6.1. Access Controls. All Apollo personnel access to the Cloud Environment is via a unique user ID and consistent with the principle of least privilege. All such access requires a VPN, with multi-factor authentication and complex passwords.

6.2. Endpoint Controls. For access to the Cloud Environment, Apollo personnel use Apollo-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 7 (Vulnerability Management).

6.3. Separation of Environments. Apollo logically separates production environments from development and testing environments. No Customer Data will be transmitted, stored or processed in a non-production environment. The Cloud Environment is both logically and physically separate from Apollo's corporate offices and networks.

6.4. Firewalls / Security Groups**.** Apollo shall protect the Cloud Environment using industry standard firewall or security groups technology to proactively set up egress and periodically review egress network traffic protocols for anomalies. Ingress is only allowed on those particular protocols and ports that are business-critical. Apollo reviews network security rulesets whenever a change is made by Apollo within the network, but in no event less than once each year.

6.5. Hardening. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Policy.

6.6. Monitoring & Logging.

6.6.1. Infrastructure Logs. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year.

6.6.2. User Logs. As further described in the Documentation, Apollo also captures logs of certain activities and changes within the Account and makes those logs available to Customer for Customer's preservation and analysis.

6.6.3. Log Maintenance. Logs that pertain to infrastructure changes are retained indefinitely and are kept in git and managed as code. Changes in infrastructure that are managed elsewhere (e.g. hosted DB version updates) are maintained for >90 days and user logs are stored for at least 30 days. Some logs are exported to analytics sinks and are stored with longer retention (>1 year).

7. **Vulnerability Detection & Management**.

7.1. Anti-Virus & Vulnerability Detection. Apollo leverages automated alerts and vulnerability reports and other threat detection tools to monitor and identify suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "**Malicious Code**"). Apollo does not monitor Customer Data for Malicious Code.

7.2. Penetration Testing & Vulnerability Detection. Apollo regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the Service at least annually. Apollo also runs weekly vulnerability scans for the Cloud Environment using updated vulnerability databases.

7.3. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Service. Upon becoming aware of such vulnerabilities, Apollo will use commercially reasonable efforts to address private and public (e.g., U.S.-Cert announced) critical and high vulnerabilities within 30 days, and medium vulnerabilities within 90 days. To assess whether a vulnerability is 'critical', 'high', or 'medium', Apollo leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

8. **Change Management**. Apollo maintains a documented change management program for the Service.

9. **Vendor Risk Management.** Apollo maintains a vendor risk management program for vendors that process Customer Data designed to ensure each vendor maintains security measures consistent with Apollo's obligations in this Security Policy.

10. **Physical and Environmental Controls**

10.1. Cloud Environment Data Centers. To ensure the Hosting Partner has appropriate physical and environmental controls for its data centers hosting the Cloud Environment, Apollo regularly reviews those controls as audited under the Hosting Partner's third-party audits and certifications. Apollo's Hosting Partner shall have a SOC 2 Type II annual audit (available at https://cloud.google.com/security/compliance/soc-2) and ISO 27001 certification (available at https://cloud.google.com/security/compliance/iso-27001) or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

10.1.1. Physical access to the facilities are controlled at building ingress points;

10.1.2. Visitors are required to present ID and are signed in;

10.1.3. Physical access to servers is managed by access control devices;

10.1.4. Physical access privileges are reviewed regularly;

10.1.5. Facilities utilize monitor and alarm response procedures;

10.1.6. Use of CCTV;

10.1.7. Fire detection and protection systems;

10.1.8. Power back-up and redundancy systems; and

10.1.9. Climate control systems.

10.2. Apollo Corporate Offices. While Customer Data is not hosted at Apollo's corporate offices, Apollo's technical, administrative, and physical controls for its corporate offices covered by its SOC 2 Type II certification, shall include, but are not limited to, the following:

10.2.1. Physical access to the corporate office is controlled at building ingress points;

10.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;

10.2.3. Visitors are required to sign in;

10.2.4. Use of CCTV at building ingress points;

10.2.5. Tagging and inventory of Apollo-issued laptops and network assets;

10.2.6. Fire detection and sprinkler systems; and

10.2.7. Climate control systems.

11. **Incident Response and Notification Procedures**.

11.1. General. For purposes of this Section, an **"Incident"** means any act or omission that compromises Apollo's or its providers' physical, technical, or organizational safeguards for the Cloud Services or that breaches this Security Policy and leads to the actual or suspected unauthorized access, use, disclosure, or processing of Customer Data. Apollo will maintain an Incident response function capable of identifying, mitigating the effects of, and preventing the recurrence of Incidents. If an Incident occurs, Apollo will (i) promptly take all necessary steps to prevent any further compromise of Customer Data or any future Incidents; (ii) notify Customer within seventy-two (72) hours (unless earlier notification is required by law) of the Incident being identified and provide updates regarding the status of the remediation at Customer's reasonable request; and (iii) respond promptly to any reasonable request from Customer for additional information pertaining to the Incident. Apollo's notice will contain a description of the known or suspected nature of the Incident, its impact, and relevant investigative, corrective, or remedial actions taken or planned (unless disclosure of the same may compromise the integrity of an ongoing

investigation or forensic analysis, in which case Apollo will share the portion of those actions taken or planned it is reasonable able to).

11.2. Audit and Reporting. Upon reasonable request, Apollo will permit Customer or its third-party auditor to review and verify relevant logs and data pertaining to any Incident investigation unless doing so impacts Apollo's ability to maintain other customer commitments concerning confidentiality and security. Upon conclusion of investigative, corrective, and remedial actions with respect to an Incident, Apollo will prepare and deliver to Customer, at its request, a final report that describes (i) the known extent of the Incident; (ii) the Customer Data subject to the Incident; (iii) all critical corrective and remedial actions completed or in process; (iv) the efforts taken to mitigate the risks of further Incidents.