⊛ ChatGPT

AWS Private Pricing Agreement *(Example Draft for Discussion)*

This Private Pricing Agreement (this "**Agreement**") is entered into as of **[Effective Date]**, by and between **Amazon Web Services, Inc.**, a Delaware corporation ("**AWS**"), and **[Customer Name]**, a [State/Country] corporation ("**Customer**"). This Agreement is an addendum to, and incorporates by reference, the AWS Customer Agreement (or other applicable master cloud services agreement) between AWS and Customer (the "**Master Agreement**"). In the event of any conflict, this Agreement will prevail with respect to the subject matter herein. AWS and Customer are each referred to as a "**Party**" and collectively as the "**Parties**."

WHEREAS, AWS is a provider of cloud computing services and Customer desires to procure such services for its enterprise operations;

WHEREAS, Customer expects to consume AWS cloud services at a significant scale and seeks cost savings and price predictability through a committed spend arrangement;

WHEREAS, AWS offers Private Pricing Agreements (also known as Enterprise Discount Programs) to high-spend customers who commit to multi-year usage in exchange for discounted pricing [1] [2] ; and

WHEREAS, the Parties have negotiated the terms of such a private pricing arrangement, including commitments by Customer and corresponding benefits from AWS, as set forth below;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained in this Agreement, and for other good and valuable consideration, the sufficiency of which is acknowledged, the Parties agree as follows:

1. Definitions

Unless defined otherwise in this Agreement, capitalized terms have the meanings given in the Master Agreement. In this Agreement, the following definitions apply:

1.1 "Annual Committed Spend" means the minimum annual dollar amount (in USD) of AWS Service usage charges (excluding taxes and after application of any AWS credits) that Customer commits to incur during each Contract Year of the Term, as set forth in Section 3.1. Annual Committed Spend amounts shall not decrease in any subsequent year of the Term [3] .

1.2 "Contract Year" means each consecutive 12-month period during the Term, with the first Contract Year beginning on the Effective Date (or a specified start date) and each subsequent Contract Year beginning on the anniversary of that date. For example, if the Term is three years, Contract Year 1 covers months 1–12, Contract Year 2 covers months 13–24, etc.

1.3 "Total Committed Spend" means the aggregate dollar amount of usage charges that Customer commits to spend over the entire Term of this Agreement. The Total Committed Spend is the sum of the Annual Committed Spend for all Contract Years.

1.4 "Discount Rate" means the percentage discount off AWS's standard pay-as-you-go service fees that is applied to Customer's usage charges for Eligible Services under this Agreement. The Discount Rate may vary by Contract Year or service, as set forth in Section 3.2. Fees for any services or accounts not covered by this Agreement remain at standard AWS rates [4] .

1.5 "Eligible Services" means the AWS Services and usage charges that are subject to the Discount Rate and that count toward the Annual Committed Spend. Unless otherwise specified, Eligible Services include the majority of generally available AWS cloud services across all AWS regions [5] , excluding any services expressly excluded in **Schedule 1** (e.g. certain new or specialized services) or as limited by AWS policy. AWS Marketplace purchases may be included toward commitment fulfillment only up to any agreed limit (e.g. a negotiated percentage) and typically are not themselves discounted [6] . *For clarity,* services or fees not included as Eligible Services (such as third-party Marketplace fees beyond the allowed portion, support fees, or other excluded items) do not count toward meeting the Committed Spend and are charged at standard rates.

1.6 "Term" means the duration of this Agreement as specified in Section 2.1, i.e. the initial committed contract period and any renewal period. This Agreement may also be referred to as the "Private Pricing Term Agreement" or "Private Pricing Addendum (PPA)" for the Term of the commitment [7] .

1.7 "Change of Control" means, with respect to a Party, any event in which a third party acquires directly or indirectly **more than 50%** of the ownership or voting securities of that Party, whether through merger, acquisition, sale of stock or assets, or other transaction, or a Party is otherwise consolidated with or into another entity. Change of Control shall not include internal reorganizations or transfers among Affiliates that do not result in a change in the ultimate controlling entity.

1.8 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party, where *"control"* means ownership of more than 50% of the voting equity or beneficial interests of the entity.

1.9 "Customer Data" (often referred to as "Your Content" in the Master Agreement) means all data, information, and content uploaded to, stored in, or processed via the AWS services by Customer or its end users, including any personal data. Customer Data does not include account information (such as contact or billing information) or any data generated by AWS about the operation or performance of the Services.

1.10 "Service Level Agreements" or "SLAs**"** means the then-current AWS service level agreements applicable to the specific AWS Services Customer uses (as published on the AWS website or provided to Customer). SLAs set forth AWS's service availability and performance commitments (e.g. uptime percentages) for those services and the corresponding service credit remedies for failure to meet such commitments [8] [9] .

1.11 "Service Credits" means the credits or financial remedies that AWS offers to Customer (usually as credits against future service use) for AWS's failure to meet an SLA performance commitment. Service

Credits are typically defined in the applicable SLA and are **Customer's sole and exclusive remedy** for the service performance or availability issue in question [9] .

(Additional definitions may be set forth elsewhere in this Agreement or in an attached schedule. Any capitalized terms not defined in this Agreement have the meanings given in the Master Agreement.)

2. Term; Renewal; Termination

2.1 Term. The Term of this Agreement shall commence on the Effective Date and continue for a period of **[Three (3)] years** ending on **[End Date]**, unless earlier terminated as provided herein (the "**Initial Term**"). This Agreement is a commitment for a multi-year term in exchange for the negotiated discounts, and neither Party may terminate this Agreement for convenience during the Initial Term [10] . This Agreement will automatically terminate upon any termination of the underlying Master Agreement between the Parties [11] , subject to Section 2.4 below.

2.2 Renewal. The Parties may mutually agree in writing to renew or extend this Agreement beyond the Initial Term (for example, to negotiate a new committed spend term). Any renewal shall be agreed at least [60] days prior to the end of the then-current Term, to allow continuity of pricing. Unless a renewal or extension is signed by both Parties, upon expiration of the Term Customer's discounts will end and AWS's standard on-demand pricing and terms will apply to Customer's continued use of AWS services. For the avoidance of doubt, this Agreement does not auto-renew by default, and any *post-term* usage of services absent a new agreement will be at standard rates (or under any new agreement the Parties execute).

2.3 Termination for Cause. Either Party may terminate this Agreement (and the Master Agreement, if applicable) for cause if the other Party materially breaches this Agreement and fails to cure such breach within thirty (30) days after receiving written notice specifying the breach. In addition, AWS may terminate this Agreement for cause immediately upon written notice if Customer fails to pay any amount due under this Agreement or the Master Agreement and such failure continues for more than fifteen (15) days past due, or if Customer is in breach of the usage restrictions or compliance requirements of the Master Agreement (such as violation of law or AWS's acceptable use policies) and fails to promptly cure upon notice. Any termination of this Agreement for cause by AWS is without prejudice to AWS's other rights and remedies. **Upon any termination for cause by AWS**, including termination of the Master Agreement or this Agreement due to Customer's breach, **AWS may charge Customer the difference between the discounted fees and the standard (undiscounted) AWS fees for all Services used by Customer under this Agreement up to the date of termination** [12] , **less** any amounts already paid by Customer (such as any true-up payments for shortfalls) (the "**Return Amount**"). In other words, Customer will lose the benefit of the discount for the usage period and must retroactively pay AWS for the discount that was previously given, to make AWS whole for Customer's failure to fulfill the committed term. AWS may immediately invoice Customer for the Return Amount upon termination. Any Annual Commitment Payments (true-up payments) made by Customer for prior Contract Years shall be credited **against** the Return Amount [12] .

If Customer terminates this Agreement for AWS's uncured material breach (and Customer is not in breach), Customer will not be responsible for any early termination penalties or Return Amount beyond paying for actual services used up to termination; in such case, if Customer had prepaid any unused portion of the Committed Spend, AWS will refund any remaining unused prepaid amount after offsetting any fees for services consumed up to termination. Except as set forth in this Section 2.3, AWS shall not be liable to Customer for any termination of services permitted under the Master Agreement (e.g. suspension or

termination for abuse or legal compliance), but any such termination will be handled in accordance with the Master Agreement's terms and the provisions of this Agreement regarding fees.

2.4 No Termination for Convenience. Customer acknowledges that it is receiving substantial pricing discounts in exchange for its multi-year commitment, and therefore Customer has **no right to terminate for convenience** or without cause during the Term. Likewise, AWS agrees that it will not terminate the Master Agreement or this Agreement for convenience during the Term [10] , and any termination must be pursuant to Section 2.3 (Cause) or Section 8 (Change of Control) or a mutual written agreement. The foregoing does not limit Customer's ability to reduce or cease usage of AWS services, but Customer will remain responsible for any shortfall fees as described in Section 3.3 even if it reduces usage (i.e. there is no early release from the committed spend except as expressly provided herein).

2.5 Effect of Expiration or Termination. Upon expiration of the Term (or any earlier termination of this Agreement), the pricing benefits and discounts under this Agreement shall cease, and Customer's continued use of AWS services (if any) will be governed by the standard pricing and terms under the Master Agreement (unless otherwise agreed in writing, such as entering into a new PPA). If this Agreement expires or terminates prior to Customer fulfilling the Total Committed Spend (e.g. in case of an early termination for cause or if Customer simply did not meet the commitment by term-end), then Section 3.3 (True-Up for Shortfalls) and Section 2.3 above (Return Amount on early termination) shall apply. **Surviving Obligations:** The provisions of this Agreement that by their nature are intended to survive (including payment obligations, confidentiality, indemnities, liability limitations, and others specified as surviving in the Master Agreement) shall survive expiration or termination. Termination or expiration shall not affect any accrued rights or liabilities of either Party up to the date of termination.

3. Pricing, Discounts and Payment

3.1 Committed Spend & Commitment Schedule. During the Term, Customer commits to meet or exceed certain minimum spending levels on AWS services. The **Annual Committed Spend** for each Contract Year is set forth in the table below. Customer's total commitment over the entire Term (Total Committed Spend) is **$ [__]**. Customer agrees that its actual AWS usage (in billed charges) in each Contract Year will equal or exceed the Annual Committed Spend for that year. Annual commitments are equal to or greater than the prior year's commitment (no reductions year-over-year) [3] . The committed amounts and corresponding discount rates are as follows:

- **Contract Year 1:** *[Dates]* – Annual Committed Spend = **$X**, with **Y%** Discount Rate on Eligible Services.
- **Contract Year 2:** *[Dates]* – Annual Committed Spend = **$X** ($\geq$ Year 1), with **Y%** Discount Rate on Eligible Services.
- **Contract Year 3:** *[Dates]* – Annual Committed Spend = **$X** ($\geq$ Year 2), with **Y%** Discount Rate on Eligible Services.

(Example above: Customer commits to $X million per year for 3 years with a Y% platform-wide discount. Actual numbers and any escalation can be inserted.)

Customer acknowledges that these commitments are firm and agrees to carefully plan its AWS usage so as to meet or exceed the committed amounts [13] [14] . **For clarity, any AWS credits or discounts provided to Customer (including the Discount Rate hereunder) do not count toward the committed spend** – Customer must still **achieve the full $ amount in actual, billable usage** [6] . Likewise, any usage covered

by prior purchases (e.g. pre-purchased Reserved Instances or Savings Plans outside this Agreement) may not count toward new commitments unless otherwise specified. However, a portion of third-party AWS Marketplace spend **may** be allowed to count toward the commitment (typically up to 25% as negotiated) [6], provided such Marketplace usage is through Customer's AWS accounts and is paid through AWS billing. Customer confirms that it has evaluated its future cloud needs and is confident in its ability to meet these spend levels [13]. Customer's AWS usage is expected to be sustained or grow over time, and commitments cannot decrease over the Term [3].

3.2 Discounted Pricing & Tiers. In consideration of Customer's commitments, AWS will apply a **Discount Rate** to Customer's charges for Eligible Services during the Term. For each Contract Year, the applicable Discount Rate is as specified in Section 3.1 above (or in **Schedule 1** if detailed by service or tier). The discount is applied as a percentage off AWS's standard pay-as-you-go rates (or off the applicable AWS price listed on the AWS Site for the service in question) for Customer's usage of Eligible Services. The discounted fees will be calculated as: **Fee = Standard AWS Fee – (Discount Rate × Standard AWS Fee)** [4]. This Discount Rate is locked in for the Contract Year for all usage of Eligible Services under Customer's covered accounts, subject to the terms below.

- **Volume/Tiered Discounts:** If the Parties have agreed on specific pricing tiers for certain services (e.g. enhanced discounts at higher usage volumes or fixed rates for certain usage bands), those will be detailed in **Schedule 1 – Pricing Details**. For example, the Parties may agree to **service-specific pricing** such as reduced rates for outbound data transfer or a larger discount on a particular high-volume service. Any such special pricing or tiered discounts will apply as expressly set forth in Schedule 1, and in the event of any inconsistency between a general Discount Rate and a service-specific rate in Schedule 1, the service-specific rate shall apply for that service. *(By way of illustration, an agreement might specify that Customer gets a platform-wide 10% discount on all services, and a 20% discount on Amazon EC2 usage above $500k/year, etc.)* Special discounts on specific services or Marketplace products may be included for large enterprise deals [15].

- **No Double Discounts / Best Price Application:** The Discount Rate under this Agreement will not "stack" with other publicly available AWS discounts for the same usage. If Customer is separately entitled to another AWS discount or incentive for a particular service usage (for example, if AWS offers a volume-based price reduction, a reserved instance or savings plan pricing, or a region-specific promotion that yields a lower effective rate than the Discount Rate would), then Customer will be charged the **lower** of (a) the price after applying this Agreement's Discount Rate, or (b) the price resulting from such other applicable discount program [16]. In other words, Customer will always receive at least the better of the two pricing outcomes, but will not receive *double* cumulative discounts. For clarity, AWS will not apply the PPA Discount Rate to any fees for which Customer is already paying a discounted or fixed rate under another arrangement (e.g. fees for an existing Savings Plan, or an existing special bid for a specific project) – those remain at their agreed rates unless otherwise agreed. Also, certain services (like Enterprise Support fees, or certain managed services) are typically excluded from platform discounts and would remain at standard rates unless explicitly discounted.

- **Changes to Services or Prices:** Customer understands that AWS's standard service offerings and pricing may change over time (for example, AWS may introduce new services, or reduce standard prices). If AWS generally reduces the public on-demand rate for a service that Customer is using, Customer will benefit from that price reduction *in addition to* the Discount Rate (since the Discount

Rate applies to the new lower base price). If AWS discontinues or materially alters an Eligible Service, AWS will, in good faith, allow Customer to apply its committed spend to equivalent or successor services or otherwise ensure Customer continues to receive comparable benefit. Any new AWS services launched during the Term are not automatically included as Eligible Services under this Agreement; however, AWS may, upon Customer's request, agree in writing to extend the Discount Rate to such new services or add them to Schedule 1 if mutually acceptable.

3.3 Billing, True-Up and Shortfall Payments. AWS will bill Customer's usage of AWS services in accordance with the standard billing cycles (typically monthly in arrears for usage charges, and in advance for any upfront fees). All invoicing and payments will be governed by the Master Agreement except as modified here. **Customer will pay invoices within [30] days** of invoice date (net 30), in accordance with the payment methods on file. All payments will be made in U.S. Dollars (USD), unless a different currency is agreed in writing.

At the **end of each Contract Year**, AWS will review Customer's actual billed usage for that year (the total "Actual Spend"). If the Actual Spend for Eligible Services in that year (excluding any usage covered by prior Annual Commitment Payments, see below) is less than the Annual Committed Spend for that Contract Year, Customer will owe a **shortfall true-up payment** for that year. Specifically, AWS will invoice Customer for an amount equal to **(Annual Committed Spend – Actual Spend)** for that year (the "**Annual Commitment Payment**") [17] . Customer shall pay such invoice within 30 days. **AWS will then apply any such true-up payment as a pre-paid credit** to Customer's AWS account for future usage: the amount paid will be applied against Customer's subsequent monthly usage charges for Eligible Services in the *next Contract Year* until the credit is exhausted [18] . (For example, if in Year 1 Customer committed to $5M but only spent $4.5M, AWS invoices $500k; once paid, that $500k is available as credit to cover usage in Year 2.) Any Annual Commitment Payment credit not used by the end of the Term will expire, and AWS will not refund any unused portion (all such payments are **non-refundable** except as applied to usage) [19] . Following the **final Contract Year**, if Customer's total Actual Spend over the Term is less than the Total Committed Spend, AWS may invoice Customer for the remaining unused commitment (after applying any interim true-ups) and designate such amount as fees for use of a specified AWS service (e.g., EC2) during the Term, solely for the purpose of finalizing the commitment usage [19] . Customer acknowledges that committing to a realistic spend level is important, as any **shortfall will be charged back at the end of the year** (or term) [14] . *Conversely*, if Customer's Actual Spend *exceeds* the Annual Committed Spend in a given year, the excess usage will simply be billed at the discounted rates as normal (there is no penalty for overachievement; however, overspend in one year does not offset a shortfall in another year). The committed spend and true-up mechanism apply separately to each Contract Year.

3.4 Pricing Adjustments for Growth: If at any time during the Term Customer significantly exceeds its projected usage growth (for example, due to a major business expansion or migration project), the Parties may discuss in good faith adjusting the committed amounts or discount levels. AWS's discount tiers are generally more favorable for larger and longer commitments [20] . Thus, if Customer wishes to **increase** its Total Committed Spend or extend the Term, AWS may offer a higher Discount Rate or other incentives for the additional commitment (subject to mutual agreement via an amendment). Any such changes must be documented in writing (e.g., an amendment or replacement agreement). Unless and until an amendment is signed, the commitments and rates in this Agreement remain in effect.

3.5 Taxes. All fees and other charges under this Agreement are **exclusive of any taxes, levies, duties or similar governmental assessments** ("**Taxes**"). Each Party is responsible for its own Taxes as required by

applicable law [21] . AWS may be required by law to collect certain Taxes (such as sales, use, value-added tax (VAT), goods and services tax (GST), or similar indirect taxes) on the services provided; if so, AWS will itemize such Taxes on the invoice and Customer agrees to pay such Taxes, unless Customer provides a valid exemption certificate or other documentation proving exemption [22] . Customer shall provide AWS with any tax identification information or exemption certificates reasonably required to ensure compliance with tax laws. **Taxes on Customer's income, net worth, or corporate existence** are the responsibility of Customer. **Taxes on AWS's income** or net income are the responsibility of AWS. If any Taxes are required to be withheld from a payment to AWS (e.g. withholding taxes imposed by a foreign jurisdiction), Customer will gross-up the payment such that AWS receives the full amount it would have received absent such withholding [23] . The Parties shall cooperate to minimize any Taxes legally due, including by completing and exchanging any necessary forms (such as IRS Form W-8 or W-9, or applicable certificates). For clarity, all amounts due under this Agreement shall be paid in full to AWS **without any set-off, deduction, or withholding**, except as expressly required by law and addressed by the gross-up mechanism above.

3.6 Invoicing and Account Structure. This Agreement's pricing applies to Customer's AWS account(s) as identified by the Parties. **Schedule 2** may list the specific AWS account IDs or linked accounts that are **Eligible Accounts** under this Agreement. Only usage under the Eligible Accounts qualifies for the discounted pricing and counts toward the commitments [4] . If Customer wishes to add or remove accounts (such as new subsidiaries or consolidated billing accounts) to this Agreement, it must obtain AWS's written approval (which shall not be unreasonably withheld for Customer's wholly-owned Affiliate accounts). All Eligible Accounts must be owned or controlled by Customer and used for Customer's internal business purposes (no reselling to third parties unless authorized in writing). Customer must ensure that all Eligible Accounts are consolidated under an AWS Organizations payer account if required for billing efficiency. AWS will invoice Customer at the payer level (master billing account) for all Eligible Account usage. All invoices shall reference this Agreement. Customer's payment obligations and AWS's rights to suspend or terminate for non-payment (per the Master Agreement) apply to any invoiced amounts under this Agreement. AWS may **offset** any service credits or SLA credits against amounts due, but will not apply discounts to the point of rendering any invoice negative (no payouts of unused discounts or credits, except as provided in true-up application).

3.7 Enterprise Support Fees. Customer acknowledges that enrollment in **AWS Enterprise Support** is required as a condition of this Private Pricing Agreement [24] [25] . Throughout the Term, Customer **shall maintain an Enterprise Support subscription** for its AWS account(s). If Customer is not enrolled in Enterprise Support for any month during the Term, AWS will automatically enroll Customer and charge the applicable Enterprise Support fees for that period [25] . Enterprise Support provides Customer with enhanced support services, including a Technical Account Manager and faster response times, which are valuable given Customer's scale and critical use of AWS. Enterprise Support fees are calculated as a percentage of AWS spend (per AWS's standard support pricing) and are **not** subject to the Discount Rate under this Agreement (support fees are typically excluded from service discount programs). However, the Enterprise Support spend **does count** toward meeting Customer's committed spend in this Agreement (since it is an AWS charge), unless AWS specifies otherwise. Customer's commitment to maintain Enterprise Support is a material obligation; failure to maintain support enrollment (or equivalent support through an authorized AWS partner, if agreed) is considered a breach of this Agreement. *(If the Parties agree to any modification of support requirements or fees, it should be stated here.)*

4. Service Levels and Support

4.1 Service Availability Commitments. AWS will use commercially reasonable efforts to make the AWS Services available to Customer in accordance with the performance standards set forth in the applicable **AWS Service Level Agreements (SLAs)** [8] . For each AWS Service that Customer utilizes which has an official SLA, AWS's obligations to meet certain uptime or response metrics and to provide Service Credits for any failures shall be governed by the terms of that SLA. AWS will provide Customer with Service Credits in accordance with the SLA if the service performance falls below the committed SLA thresholds. **Any Service Credits earned will be applied to Customer's future invoices for that service** (or paid out pursuant to the SLA terms) and are **the sole and exclusive remedy** for the covered service level failures [9] . Customer acknowledges that AWS's standard SLA remedies (typically service credits) are adequate and sufficient compensation for service availability issues, and Customer will not pursue additional remedies for such issues absent a separate written agreement. If a service that Customer uses does **not** have a published SLA, AWS will endeavor to provide a level of service support consistent with industry standards and with its treatment of similarly situated enterprise customers, but no specific uptime guarantee is given for services without an SLA.

4.2 Support Services. AWS will provide Customer with **Enterprise Support** throughout the Term (as noted in Section 3.7). Under Enterprise Support, AWS shall assign a **Technical Account Manager (TAM)** or similar resource to Customer's account and provide 24/7 access to AWS's support engineers for technical assistance. AWS will respond to Customer's support cases according to the response times associated with Enterprise Support severity levels (e.g. **<15 minute** response for critical **Severity 1** issues). Additional details on support scope (architectural reviews, operation reviews, training, etc.) are described in AWS's Enterprise Support plan documentation. AWS will also engage in **operational reviews** and business reviews with Customer periodically (e.g. quarterly) to discuss Customer's usage, costs, and any optimization or architectural guidance. *While Enterprise Support is generally provided under AWS's standard terms, the Parties may attach a Support Services Exhibit if any custom support obligations (e.g. dedicated support personnel, on-site support, etc.) have been agreed.* Any such special support terms would be in **Schedule 3**.

Notwithstanding any enhanced support, Customer remains responsible for designing and maintaining its applications to be resilient and for following AWS best practices. AWS does not guarantee that it can resolve every issue immediately, but will use diligent efforts in line with its Enterprise Support commitments. The fees for Enterprise Support are as set forth in Section 3.7 and are billed separately from service usage fees.

4.3 Service Level Reporting and Credits. At Customer's request, AWS will provide reports detailing AWS's performance against applicable SLA metrics for Customer's services (or Customer can access service health dashboards and Personal Health Dashboard for real-time info). If Customer believes it is entitled to a Service Credit under an SLA, Customer should submit an SLA claim to AWS support within the time frame specified by that SLA (typically within 30 or 60 days of the outage incident). AWS will review the claim and, if validated, will issue the corresponding credit to Customer's account. Service Credits have no cash value and can only be used toward future service billings, and they expire if not used within the stipulated period (per the SLA or AWS policy). Service Credits cannot be applied to the committed spend obligation (i.e., they don't reduce the commitment amount; they are a remedy for performance issues). Other than providing Service Credits, AWS has no further liability for failing to meet an SLA, **except** that if AWS were to *grossly* or continually fail to meet core service uptime commitments such that it fundamentally fails to deliver the services as contracted, such failure may constitute a material breach under Section 2.3 (entitling Customer to terminate for cause if not cured).

5. Usage Forecasts and Governance

5.1 Capacity Forecasts. To facilitate efficient capacity planning and to ensure AWS can meet Customer's needs, Customer agrees to provide AWS with **periodic usage forecasts**. Specifically, Customer will, in good faith, provide AWS with a **rolling [quarterly] forecast** of its anticipated AWS usage and spend, broken down by major service categories (compute, storage, database, etc.) or as reasonably requested by AWS. Forecasts are non-binding estimates for planning purposes, but should be as realistic and accurate as possible [13] . Initially, Customer's projected usage that informed this Agreement is attached as **Schedule 4 (Usage Forecast)** for the Term. Going forward, Customer will update AWS (for example, during quarterly business reviews) on any significant changes in its expected consumption. If Customer anticipates a **significant increase** in usage (beyond what was originally projected) – for instance, a major migration event or new application launch – Customer will inform AWS at least [60] days in advance, to allow AWS to ensure adequate infrastructure is available. Likewise, if Customer foresees any risk of **shortfall** in usage relative to the commitment (e.g., due to business downturn or project delays), Customer shall promptly notify AWS so that the Parties can discuss possible mitigations (such as scope adjustments, marketing credits, or other strategies). The Parties acknowledge that accurate forecasting is crucial to avoiding overcommitment or unexpected costs [13] .

5.2 Governance and Business Reviews. The Parties shall maintain open communication regarding Customer's AWS utilization. At least on a **quarterly basis**, AWS and Customer will conduct a governance meeting (in-person or via conference) to review: (a) Customer's actual usage and spend versus the commitment targets; (b) any operational issues or service performance matters; (c) upcoming projects or changes that may affect usage; and (d) opportunities for cost optimization or architectural improvements. AWS may provide tools or reports (such as AWS Cost Explorer or third-party tools) to help Customer in tracking and forecasting usage. If Customer's actual usage is trending behind the committed pace, AWS may offer guidance or assistance (for example, identifying additional workloads that could be moved to AWS) to help Customer realize the expected value of the Agreement. Both Parties will cooperate in good faith to achieve the intended benefits of this Agreement – cost savings for Customer and sustained usage for AWS. *Nothing in this Section 5 imposes a penalty on Customer for deviating from forecasts (commitment obligations are governed by Section 3), but regular forecasting and communication are encouraged to prevent issues.*

5.3 Flexibility for Changing Requirements. AWS understands that Customer's business needs may evolve. If Customer undergoes a business event significantly impacting its AWS usage (such as a merger, divestiture, or change in strategy), Customer may request a meeting with AWS to discuss potential modifications to the remaining commitment or scope. While AWS is not obligated to modify the commitment, AWS will reasonably consider adjustments that maintain a mutually beneficial arrangement (for instance, repurposing unused commitment toward new services or extending the term to allow more time for consumption). Any adjustments must be documented by written amendment. Unless and until such amendment is signed, the original terms remain in force.

6. Data Residency, Security, and Privacy

6.1 Data Residency and Location Controls. Customer may specify the AWS region(s) in which its Customer Data is stored and processed, by selecting particular AWS geographic regions when configuring resources. AWS will not move Customer Data from the regions selected by Customer, nor disclose Customer Data to any government or third party, **except** as necessary to maintain or provide the services or as required by

law or a binding governmental order [26] . In the event that AWS is legally required by a valid order (such as a subpoena or court order) to disclose or move Customer Data (e.g. to a governmental authority), AWS will, to the extent legally permitted, give Customer **notice** of the requirement so that Customer may seek a protective order or other remedy [27] . AWS will not transfer Customer Data outside of the chosen regions except to the extent necessary for AWS to comply with law or to provide the Service Offerings (for example, certain account administrative or billing data may be processed in the United States as part of AWS's global operations, or metadata and service attributes as described in the AWS Agreement) [26] . AWS confirms that aside from such limited exceptions, all Customer Data will remain within the AWS data centers in the regions that Customer has selected for its resources. AWS also agrees that it will abide by any specific data residency requirements mutually agreed in writing (for instance, if **Customer requires that all data remain within the EU** to comply with EU data protection laws, AWS shall ensure the services are configured to meet that requirement in conjunction with Customer's use of regional selection).

6.2 Data Privacy and Processing. AWS will handle Customer Data in accordance with the **AWS Data Privacy terms** in the Master Agreement and the AWS Data Processing Addendum ("DPA") that addresses GDPR and other data protection laws [28] . The AWS DPA (available on AWS's website) is hereby incorporated by reference, and AWS confirms it will process any personal data contained in Customer Data only in accordance with Customer's documented instructions (as provided through Customer's use and configurations of the services) and consistent with the DPA [28] . AWS acts as a **"data processor"** (or "service provider") for most Customer Data, and Customer remains the **"data controller"** (or "business") determining the purposes of processing. AWS will implement and maintain appropriate technical and organizational measures to protect personal data, as detailed in the AWS DPA and security documentation. This includes measures such as encryption at rest and in transit (where configured), access controls, security monitoring, and regular security assessments. AWS also commits to assisting Customer in complying with certain data subject rights or regulatory requests, to the extent AWS is able as a processor (for example, by enabling Customer to delete or retrieve data, or by providing certifications of compliance). If Customer needs to execute a separate copy of the AWS DPA for its records or compliance, AWS will promptly do so upon request. Additionally, if Customer requires a **Business Associate Addendum (BAA)** for HIPAA compliance (in case Customer will store protected health information on AWS), AWS will provide and honor its standard BAA as part of this Agreement. AWS represents that as of the Effective Date, it has in place a Global Data Processing Addendum that meets the requirements of the EU General Data Protection Regulation (GDPR) and similar laws, including Standard Contractual Clauses for cross-border data transfers, which AWS will abide by when applicable. Customer is responsible for its own compliance with privacy laws as a controller, including providing any required notices and obtaining any necessary consents from data subjects for use of AWS services.

6.3 Security Measures. AWS will maintain a robust security program for its cloud infrastructure. **AWS Security:** AWS shall implement and maintain **reasonable and appropriate administrative, physical, and technical safeguards** designed to secure Customer Data against unauthorized access, loss, or disclosure, in accordance with industry best practices [29] . Without limiting the foregoing, AWS will (a) ensure its data centers and services employ strong physical security and access controls; (b) implement network security measures (firewalls, intrusion detection, encryption for data in transit, etc.); (c) regularly test and evaluate the effectiveness of its security measures; and (d) undergo third-party audits/certifications of its security (such as SOC 1, SOC 2, and ISO 27001 certifications) [30] . AWS currently maintains a broad set of security and compliance certifications, including ISO/IEC 27001, 27017, 27018, and others, as well as adherence to frameworks like PCI-DSS, FedRAMP, and HIPAA where applicable [30] . Upon Customer's request, AWS will provide or make available (e.g., through AWS Artifact) its current certifications and audit reports so that

Customer can verify AWS's compliance posture. AWS will also comply with the **AWS Security Standards** and obligations set forth in the Master Agreement (which include not accessing Customer Data except to provide the services or as required by law, and implementing measures to protect data) [26] . **Security Incidents:** In the event AWS becomes aware of any **Security Incident** (meaning unauthorized access to Customer Data stored in AWS's systems resulting in actual or likely compromise of the confidentiality, integrity, or availability of such data), AWS will promptly notify Customer and will investigate and remediate the incident in accordance with AWS's incident response policies and any applicable law. AWS will keep Customer informed of developments and reasonably cooperate with Customer's own incident response efforts (e.g., providing information needed for Customer to fulfill any reporting obligations). Both Parties shall each be responsible for their respective obligations under data breach notification laws.

6.4 Customer's Security Responsibilities. Customer remains responsible for the security of its AWS accounts and its applications/configurations **within** the AWS environment (the so-called "**cloud shared responsibility**" model). Customer must use proper access keys and credentials, apply encryption and backups as appropriate, and generally follow AWS's best practice guidelines (e.g., the AWS Well-Architected Framework) to secure what it builds on AWS [31] [32] . AWS shall not be liable for any security issues or data breaches to the extent caused by Customer's own negligence or misuse of the Services, such as failing to secure login credentials, misconfiguring services to be public, or ignoring security advisories. That said, AWS will notify Customer of any critical security patches or known vulnerabilities in the AWS services that require Customer action, if AWS becomes aware (for example, via the AWS Security Bulletins or Personal Health Dashboard). Customer should promptly apply any recommended patches or mitigations to maintain a secure environment.

6.5 Data Access and Indemnity. AWS will not access Customer Data except as necessary to provide support or resolve issues (with Customer's authorization through support cases) or as otherwise legally compelled. If AWS personnel do access Customer Data for such purposes, they will be bound by confidentiality obligations. Customer shall indemnify AWS for any third-party claims arising from Customer's encryption or security measures (or lack thereof) in Customer's use of the services, **except** to the extent the claim is caused by AWS's breach of its obligations in this Section 6. *(This is further covered in Section 7 on indemnities.)*

7. Indemnification

7.1 Indemnification by AWS. AWS will defend Customer and its officers, directors, and employees (the "Customer Indemnified Parties") against any third-party claim alleging that the AWS Services (when used as authorized under the Master Agreement) **infringe or misappropriate** that third party's patent, copyright, trademark, or trade secret rights, and AWS will pay the amount of any **adverse final judgment or settlement** agreed to by AWS resulting from such claim [33] . This AWS indemnity is conditioned on Customer (i) promptly notifying AWS in writing of the claim, (ii) giving AWS sole control of the defense and any settlement negotiations, and (iii) cooperating with AWS (at AWS's expense) in the defense. AWS will not be responsible for any compromise or settlement made without its consent. In the event of any such IP infringement claim, AWS may, at its option, either: (a) procure for Customer the right to continue using the affected Service; (b) modify or replace the Service to be non-infringing while providing substantially equivalent functionality; or (c) if options (a) and (b) are not reasonably available, terminate the affected Service or feature and (if Customer is actually prevented from using the Service due to the claim) provide a pro-rata refund of any pre-paid fees for the terminated portion of the Service. AWS shall have no indemnification obligation for any claims to the extent arising from: Customer's content or application

running on the Services; Customer's breach of the Agreement; modifications to the Service by Customer or third parties not authorized by AWS; or use of the Service in combination with products not provided by AWS (if the claim would have been avoided by not such combination). **This Section 7.1 states AWS's entire liability, and Customer's exclusive remedy, for any claim of intellectual property infringement or misappropriation by the AWS Services.**

7.2 Indemnification by Customer. Customer will defend, indemnify, and hold harmless AWS, its Affiliates, and their officers, directors, employees, and licensors (the "AWS Indemnified Parties") from and against any **claim, demand, lawsuit or proceeding** brought by a third party alleging: (a) that **Customer's or any End User's use of the AWS Services** (including any activities under Customer's AWS accounts) **violates the law, regulation, or the rights of any third party** (for example, claims related to unauthorized use of data, or alleged illegal content stored by Customer) [34] ; (b) that **Customer's breach** of this Agreement or the Master Agreement has caused harm to the third party (including any breach of the Acceptable Use Policy or data protection laws by Customer) [35] ; or (c) any claim involving **Customer Data or other content** provided by Customer, including any claim that Customer Data (when used as permitted) infringes or misappropriates a third party's intellectual property or privacy rights [36] . Customer will indemnify the AWS Indemnified Parties from any **damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees)** finally awarded or agreed to in settlement for such claims. Customer's obligations are conditioned on AWS (i) promptly notifying Customer of the claim (provided that failure to do so only relieves Customer of responsibility to the extent materially prejudiced), (ii) giving Customer sole authority to defend or settle the claim (except Customer shall not settle any claim that imposes liability or admission of fault on AWS without AWS's consent), and (iii) providing reasonable cooperation at Customer's expense. AWS may, at its own cost, participate in the defense with counsel of its choosing, but Customer will have control.

7.3 Indemnification Process and Additional Terms. In any indemnified claim under Section 7.1 or 7.2, the **indemnifying Party** (AWS under 7.1, Customer under 7.2) shall have full control of the defense and settlement of the claim, provided that: (a) the indemnified Party (AWS or Customer, as applicable) may, at its own expense, participate in the defense with its own counsel; and (b) the indemnifying Party will not agree to any settlement that requires an admission of fault or payment by the indemnified Party without that Party's prior written consent (which shall not be unreasonably withheld). The indemnified Party shall provide timely notice of any claim, furnish promptly to the indemnifying Party all relevant facts and documents within its control, and reasonably cooperate (at the indemnifying Party's expense) in the defense. Failure to promptly notify only relieves the indemnifier of its obligations to the extent it is materially prejudiced by the delay [37] . The indemnifying Party shall not be liable for any legal fees or expenses incurred by the indemnified Party without the indemnifier's prior consent. The remedies in this Section 7 (defense and payment of judgments/settlements) are in lieu of any implied indemnity or similar rights, and, **subject to any limitations of liability** in the Master Agreement, each Party's indemnification obligations are capped to the same extent as other liabilities (unless otherwise provided in the Master Agreement or this Agreement).

(For example, if the Master Agreement limits AWS's total liability, that may also apply to AWS's indemnity obligations, except typically IP indemnity might be carved out from certain caps. The specifics should align with the Master Agreement's liability section.)

8. Change of Control and Assignment

8.1 Notice of Change of Control. Customer shall provide AWS with **prompt written notice** (within 30 days) in the event of any Change of Control of Customer. Likewise, AWS will inform Customer (via public announcement or direct notice) if AWS undergoes a Change of Control, to the extent such event is not publicly known. Such notices are for informational purposes and to facilitate discussions under Section 8.2, if applicable.

8.2 Change of Control – Rights and Termination. In the event Customer undergoes a Change of Control, AWS's willingness to continue the Agreement may depend on the nature of the acquiring entity. **If the acquiring or controlling entity of Customer is a direct competitor of AWS's cloud services business** (for example, an established large-scale cloud infrastructure provider), AWS may **object** to the assignment of this Agreement to such entity. AWS shall notify Customer in writing within 60 days of receiving Customer's Change of Control notice if it believes the new controlling entity is a competitor. In such case, AWS and Customer will discuss in good faith whether adequate safeguards (such as information firewalls) can be implemented to continue the relationship. If no mutually acceptable solution is reached, AWS may elect to **terminate this Agreement upon 30 days' notice** without penalty. In the event of such termination, Customer will be relieved of any future commitments beyond the effective termination date, but will remain liable for any accrued but unpaid fees and any shortfall amounts for any completed Contract Year prior to termination. If AWS does not object within the 60-day period, or if the new owner is not an AWS competitor, then this Agreement will continue in effect and the successor will be bound as the Customer. AWS shall not unreasonably refuse to continue the Agreement with a successor that is not a direct competitor or that agrees to reasonable mitigating measures.

Conversely, if AWS undergoes a Change of Control (e.g., AWS is acquired or spun off from Amazon.com, Inc.), Customer shall have the right to terminate this Agreement for convenience if the successor entity is unacceptable to Customer *in a reasonable, good-faith determination*. Customer must exercise any such termination right by written notice to AWS within 90 days of public announcement of the Change of Control. If Customer elects termination under this provision, any remaining commitment true-up obligations for the then-current year will be waived (on a pro rata basis from termination date), and Customer will pay only for actual usage up to termination. However, Customer will forfeit any future discounts under the Agreement from the termination date onward. This Section is intended to protect Customer from being locked into a contract if AWS's corporate ownership fundamentally changes in a way that impacts AWS's ability to perform or Customer's regulatory requirements.

8.3 Assignment. Except in connection with a permitted Change of Control as described above, **neither Party may assign or transfer this Agreement, in whole or in part, without the prior written consent of the other Party**, which shall not be unreasonably withheld. Any attempted assignment in violation of this clause is void. Notwithstanding the foregoing, either Party may assign this Agreement, in its entirety, without consent: (a) to an Affiliate, provided that the assigning Party remains liable for the Affiliate's performance, or (b) in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets or equity, so long as the successor agrees in writing to assume all obligations of the assignor. AWS may also assign this Agreement without consent to any AWS contracting entity that operates the AWS services in Customer's region (for example, if AWS restructures so that a local AWS entity is the service provider, AWS may assign to that entity) – in such case AWS will remain responsible for ensuring the same terms are provided. This Agreement will bind and inure to the benefit of the Parties, their respective successors, and permitted assigns.

9. Regulatory and Legal Compliance

9.1 Mutual Compliance with Laws. Each Party shall comply with all **applicable laws and regulations** in connection with its performance or exercise of rights under this Agreement. This includes, without limitation, laws relating to data privacy, export control, economic sanctions, anti-bribery (e.g. the U.S. FCPA and UK Bribery Act), employment laws for personnel, and any laws specific to the industry of Customer's use of the services. Customer is responsible for ensuring that its use of AWS services (including the content it stores and how it configures the services) complies with all laws applicable to Customer's business, such as privacy laws, consumer protection laws, and regulatory requirements in its sector. AWS shall comply with laws applicable to AWS as a cloud service provider, including maintaining any required licenses or certifications to provide the services.

9.2 Export Controls and Sanctions. Customer shall not use, export, re-export, or transfer any AWS services or software in violation of **export control or sanctions laws** of the United States or any other relevant jurisdiction [38] . Customer represents that it is not named on any U.S. government denied-party list, and it will not allow access to AWS services in embargoed countries or to prohibited parties (as of the Effective Date, AWS services may not be used in countries like North Korea, Syria, Iran, Cuba, Crimea region, or others restricted by U.S. law). Without limiting the foregoing: Customer shall not upload or transfer any data or software that is regulated under the U.S. International Traffic in Arms Regulations (ITAR) or similar regimes to AWS without prior written consent and arranging proper handling with AWS. Customer is solely responsible for compliance related to its content and use of the services, including classification of data and obtaining any required authorizations for export [39] . AWS will provide, upon request, information reasonably necessary for Customer to complete any export compliance analysis (such as identification of the export classification of AWS's products). AWS represents that to the best of its knowledge, providing the services to Customer as contemplated is not prohibited by applicable export/sanctions laws; if this changes or if a government order restricts AWS from providing services, AWS will notify Customer and may terminate or suspend services as needed to comply with law, without breach.

9.3 Industry-Specific Regulations. Customer acknowledges that AWS is a general-purpose cloud provider and is not designed to be compliant with all specific regulations that may apply to Customer (outside of those AWS officially supports). For example, AWS offers compliant solutions for many regimes (such as HIPAA, PCI-DSS, FedRAMP, GDPR, etc.), but it is Customer's responsibility to configure and use the services in a compliant manner. If Customer is in a regulated industry (healthcare, finance, government, etc.) and requires AWS to comply with specific regulatory requirements, the Parties will work together to document such requirements. For instance, if a **Business Associate Addendum** is needed for HIPAA, AWS will sign its standard BAA as noted in Section 6.2. If Customer needs AWS to maintain certain government security authorizations (e.g. FedRAMP Moderate or High for U.S. government data, or compliance with CJIS for criminal justice data), Customer should disclose this requirement. AWS has a dedicated compliance program and holds numerous certifications and attestations (SOC 1, SOC 2, ISO 27001, PCI DSS, etc.) [30] which can assist Customer in its compliance obligations. AWS will maintain those certifications relevant to the services Customer uses, to the extent generally offered to AWS customers. AWS will notify Customer if any critical certification or compliance program is lapsed or revoked during the Term, to allow Customer to assess impact. Customer may request to review AWS's audit reports and compliance documentation (under NDA if not publicly available) to verify AWS's controls.

9.4 Changes in Law or Regulation. If during the Term a change in any applicable law or regulation (or a new interpretation of existing law) materially affects the ability of either Party to perform its obligations

under this Agreement, or makes the material provisions of this Agreement illegal or unenforceable, the Parties will engage in good faith negotiations to amend the Agreement appropriately in light of the new law. Such amendments might include, for example, modifications to data handling procedures, security controls, or location of data processing. If the Parties are unable to reach agreement on necessary amendments within a reasonable period (e.g. 60 days from notice of the law change), then either Party may terminate the affected Services or this Agreement **upon written notice** without penalty. In such case, if the termination is due to a legal prohibition on AWS providing the services, AWS will refund any prepaid amounts for services not provided; if termination is due to a prohibition on Customer's use of services, Customer will remain liable for any usage up to termination but any future commitment will be released. The Parties will cooperate to wind down services in compliance with law. This Section is not intended to excuse a Party from complying with law, but to provide a mechanism to adjust the contractual relationship fairly if external legal changes disrupt the original expectations.

9.5 Regulatory Inquiries and Audit Rights. If a regulator or government authority responsible for Customer's compliance (for example, a financial services regulator or data protection authority) requests an audit or information regarding the services AWS provides to Customer, AWS will reasonably cooperate with such request to the extent it relates to AWS's role (and provided it does not violate AWS's security or confidentiality obligations to other customers). Any on-site inspections must be coordinated with AWS in advance and are subject to AWS's security policies. AWS may require such regulators to conduct audits under AWS's supervision or through third-party auditors to avoid disruption. AWS regularly undergoes third-party audits and can share those reports as a primary means of satisfying audit requirements. To the extent any direct audit of AWS by Customer or its auditor is necessary (e.g., required by law or regulators), it shall be conducted on reasonable advance notice, during normal business hours, no more than once annually, and subject to confidentiality and safety protocols. Customer will be responsible for any third-party audit costs. AWS agrees to address any significant findings from such audits in a timely manner or inform Customer of remediation plans.

10. Miscellaneous

10.1 Confidentiality. The Parties acknowledge that in the course of their business relationship, each Party may have access to information that is confidential to the other, including but not limited to business plans, technical know-how, pricing information, and Customer Data ("**Confidential Information**"). The terms and pricing of this Agreement (including the discount percentages and committed spend amounts) are **Confidential Information** of AWS and **shall not be disclosed** by Customer to any third party except: (i) to those of Customer's officers, employees, attorneys, or advisors with a need to know for purposes of implementing or enforcing this Agreement and who are bound by confidentiality obligations; (ii) as required by law or regulation (in which case Customer shall give AWS prompt notice and cooperate in seeking protective order if possible); or (iii) with AWS's prior written consent [40] . AWS likewise agrees to keep confidential any of Customer's non-public information it learns in the course of performance (including Customer's business information and any sensitive data not covered by other agreements), and will only use Customer's Confidential Information to perform its obligations or exercise rights under the Agreement. The Master Agreement's confidentiality provisions (if any) shall apply to this Agreement and information exchanged under it. Confidential Information does not include information that is independently developed by the receiving Party, is lawfully known to or obtained by the receiving Party without restriction, or that becomes public through no fault of the receiving Party. Each Party will implement reasonable measures to protect the other's Confidential Information and will not use or disclose it except as permitted herein. **Injunctive Relief:** The Parties acknowledge that unauthorized use or disclosure of Confidential Information

may cause irreparable harm, and that the injured Party shall be entitled to seek immediate injunctive relief, in addition to any other available remedies, in the event of breach of this Section. This confidentiality obligation survives for a period of at least **five (5) years** after termination of the Agreement, or indefinitely with respect to trade secrets and Customer Data.

10.2 Entire Agreement; Amendment. This Agreement, together with the Master Agreement and any schedules, exhibits, or addenda referenced herein, constitutes the **entire agreement** between AWS and Customer with respect to the subject matter (custom pricing and related commitments), and supersedes all prior or contemporaneous negotiations, discussions, or agreements, whether written or oral, regarding the same subject. The Parties acknowledge that they have not relied on any representations, warranties, or statements not expressly set forth in this written Agreement. In entering this Agreement, Customer confirms it has carefully analyzed its cloud usage and finds the commitments reasonable [13] . **Amendment:** This Agreement may only be modified or amended by a written instrument signed by authorized representatives of both Parties, except that AWS may update its standard Service Terms, Policies, or SLAs as described in the Master Agreement (provided such updates do not materially reduce the benefits under this PPA). No usage of trade, course of dealing, or course of performance will modify the express terms of this Agreement.

10.3 Order of Precedence. In the event of any conflict or inconsistency between this Agreement and the Master Agreement or other incorporated terms, **this Agreement shall control** with respect to the subject matter of pricing, commitments, and any specific provisions here that override the standard AWS terms. For matters not expressly addressed by this Agreement, the Master Agreement (including AWS's online terms, policies, and service terms) will govern. If there is a conflict between the main body of this Agreement and any Schedule or Exhibit hereto, the main body shall govern unless the Schedule expressly indicates an intent to override. If Customer has a separately negotiated enterprise agreement with AWS, this PPA is considered an addendum to that agreement.

10.4 Governing Law and Dispute Resolution. This Agreement is governed by the **laws of the State of Washington, USA**, excluding its conflict of law principles [41] . The Parties agree to submit to the exclusive jurisdiction of the federal or state courts located in King County, Washington for resolution of any disputes arising out of or relating to this Agreement, except that either Party may seek injunctive relief in any appropriate jurisdiction to protect its intellectual property or Confidential Information. The Parties expressly disclaim application of the United Nations Convention on Contracts for the International Sale of Goods and any local adoption of the Uniform Computer Information Transactions Act (UCITA) to this Agreement. *If the Master Agreement contains an arbitration clause or different governing law (e.g. based on Customer's location), those provisions shall apply instead to this Agreement to remain consistent.* In any dispute, the prevailing Party shall be entitled to recover its reasonable attorneys' fees and costs from the other Party, in addition to any other relief awarded.

10.5 Limitation of Liability. The Master Agreement's provisions on limitation of liability shall apply to this Agreement. In the absence of such provisions, the Parties agree that **neither Party shall be liable for any indirect, consequential, special, or punitive damages**, or lost profits, even if advised of the possibility of such damages, arising out of or relating to this Agreement. AWS's total cumulative liability under this Agreement (together with its liability under the Master Agreement for the same events) shall be limited to **the amount paid by Customer to AWS under this Agreement in the 12 months preceding the claim** (or the committed amount for one year, if greater). However, these limitations do **not** apply to (i) liabilities arising from willful misconduct or gross negligence, (ii) Customer's payment obligations (i.e., amounts owed

to AWS), or (iii) either Party's obligations under Section 7 (Indemnification) or breach of Section 10.1 (Confidentiality), which shall be uncapped except as may be provided in the Master Agreement. The Parties acknowledge that the pricing and commitments reflect the allocation of risk and the limitation of liability set forth herein.

10.6 Force Majeure. Neither Party will be liable for any delay or failure to perform its obligations (except payment obligations) under this Agreement if such delay or failure is due to the occurrence of events beyond its reasonable control, which may include, but are not limited to, acts of God, natural disasters (e.g. earthquakes, floods), fire, epidemic or pandemic, acts of government or regulatory authorities, war, terrorism, civil unrest, strikes or other labor disturbances, or interruptions of power or telecommunications (each, a "Force Majeure Event"). The affected Party shall promptly notify the other of the Force Majeure Event and make reasonable efforts to mitigate its impact. If a Force Majeure Event continues for a period of more than [60] days, either Party may terminate the affected services upon written notice without further liability (except that Customer will pay for services actually used prior to termination). This Section does not excuse Customer from payment for services already rendered, nor does it excuse AWS from providing service credits for outages as per SLAs (unless the Force Majeure Event falls under an SLA exclusion).

10.7 No Waiver. The failure of either Party to enforce any provision of this Agreement or to exercise any right or remedy shall not be deemed a present or future waiver of such provision, right, or remedy. The express waiver by a Party of any breach or default by the other Party shall not constitute a waiver of any different or subsequent breach or default. All waivers must be in writing and signed by the Party waiving its rights.

10.8 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, illegal, or unenforceable, that provision shall be enforced to the maximum extent permissible to effect the intent of the Parties, and the remaining provisions of this Agreement will remain in full force and effect. The Parties will negotiate in good faith a valid and enforceable provision that is as close as possible to the original intent of the invalid provision.

10.9 Independent Contractors. The relationship of AWS and Customer is that of independent contractors. Nothing in this Agreement is intended to create any partnership, joint venture, agency, or employment relationship between the Parties. Neither Party is an agent of the other nor has the authority to bind the other in any way. Each Party remains responsible for its own expenses, employees, and operations.

10.10 Notices. All notices required or permitted under this Agreement shall be given in writing and delivered to the respective addresses of the Parties as specified below (or such other address as a Party designates by notice). Notices shall be deemed given: (i) when delivered by hand (with written confirmation of receipt), (ii) when delivered by a nationally recognized overnight courier (with tracking confirmation), or (iii) when sent by email to the designated legal notice email of a Party, provided that a hard copy is also sent by one of the foregoing methods. Notices to AWS shall be sent to **Amazon Web Services, Inc., Attn: Legal Department,** [address], email: [legal-notice@amazon.com], and notices to Customer shall be sent to **[Customer Name, Attn: Legal Dept]** at the address on file or the address below, email: [___]. Routine operational communications (e.g., support tickets, usage reports) may be sent via standard electronic means and do not constitute formal notices modifying this Agreement.

10.11 Signature and Counterparts. This Agreement may be executed in counterparts (including via electronic signature or digital signing platform), each of which will be deemed an original and all of which

together will constitute one and the same instrument. The Parties agree that electronic signatures (via DocuSign or similar) or scanned copies of executed counterparts are acceptable and enforceable.

10.12 Headings; Interpretation. Headings in this Agreement are for reference only and shall not affect the interpretation of the provisions. Terms such as "including" shall be interpreted to mean "including without limitation." This Agreement was negotiated by the Parties and shall not be construed against either Party as the drafter. All schedules and attachments referenced in this Agreement are incorporated as integral parts of the Agreement. In the event of any ambiguity or question of intent or interpretation, this Agreement shall be construed as if drafted jointly by both Parties.

10.13 Authority. Each Party represents and warrants that the person signing below on its behalf has full authority to enter into this Agreement and bind the Party to its terms, and that upon execution, this Agreement is a legal, valid and binding obligation of that Party, enforceable in accordance with its terms.

The Parties have caused this AWS Private Pricing Agreement to be executed by their duly authorized representatives as of the Effective Date.

Amazon Web Services, Inc. (AWS)
By: _____ *(Authorized Signature)*
Name: _____
Title: _____
Date: _____

[Customer Name] (Customer)
By: _____ *(Authorized Signature)*
Name: _____
Title: _____
Date: _____

---

1 3 5 6 13 14 24 The Ultimate Guide to AWS PPA: PPA vs EDP, Best Practices & More | nOps
https://www.nops.io/blog/the-ultimate-guide-to-aws-ppa/

2 7 15 Anatomy of an AWS PPA Enterprise Agreement | NPI
https://www.npifinancial.com/smartspend-bulletins/anatomy-of-an-aws-enterprise-agreement

4 10 11 12 16 17 18 19 25 40 Exhibit
https://www.sec.gov/Archives/edgar/data/1576914/000162828017007056/exhibit421-mixawsaddenduma.htm

8 21 22 23 26 27 29 31 32 34 35 36 37 38 39 41 Exhibit
https://www.sec.gov/Archives/edgar/data/1576914/000162828017007056/exhibit420-awscustomeragre.htm

9 Amazon Compute Service Level Agreement - AWS
https://aws.amazon.com/compute/sla/

20 AWS EDP & PPA 2025 Negotiation Guide | CloudForecast
https://www.cloudforecast.io/blog/aws-edp-guide/

[28] AWS GDPR Data Processing Addendum – Now Part of Service Terms

https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/

[30] Cloud Compliance - Amazon Web Services (AWS)

https://aws.amazon.com/compliance/

[33] Amazon Web Services adds IP protection while dropping controversial patent clause from user agreement – GeekWire

https://www.geekwire.com/2017/amazon-web-services-added-ip-protection-dropping-controversial-patent-clause-user-agreement/