AWS Service Terms

Last Updated: November 19, 2024

1. Universal Service Terms (Applicable to All Services)

The Service Terms below govern your use of the Services. Capitalized terms used in these Service Terms but not defined below are defined in the AWS Customer Agreement or other agreement with us governing your use of the Services (the "Agreement"). For purposes of these Service Terms, "Your Content" includes any "Company Content" and any "Customer Content," and "AWS Content" includes "Amazon Properties."

1.1. You may not transfer outside the Services any software (including related documentation) you obtain from us or third party licensors in connection with the Services without specific authorization to do so.

1.2. You must comply with current technical documentation applicable to the Services (including applicable user, admin, and developer guides) posted on the AWS Site at https://docs.aws.amazon.com/index.html (and any successor or related locations designated by us).

1.3. You will provide information or other materials related to Your Content (including copies of any client-side applications) as reasonably requested by us to verify your compliance with the Agreement. You will reasonably cooperate with us to identify the source of any problem with the Services that we reasonably believe may be attributable to Your Content or any end user materials that you control.

1.4. In connection with your use of the Services, you are responsible for maintaining licenses and adhering to the license terms of any software you ru
reasonably believe any of Your Content violates the law, infringes or misappropriates the rights of any third party, or otherwise violates a material ter
Agreement (including the Service Terms, or the Acceptable Use Policy) ("Prohibited Content"), we will notify you of the Prohibited Content and may re
that such content be removed from the Services or access to it be disabled. If you do not remove or disable access to the Prohibited Content within 2 business

days of our notice, we may remove or disable access to the Prohibited Content or suspend the Services to the extent we are not able to remove or disable access to the Prohibited Content. Notwithstanding the foregoing, we may remove or disable access to any Prohibited Content without prior notice in connection with illegal content, where the content may disrupt or threaten the Services or in accordance with applicable law or any judicial, regulatory or other governmental order or request. In the event that we remove Your Content without prior notice, we will provide prompt notice to you unless prohibited by law. We terminate the accounts of repeat infringers in appropriate circumstances.

1.5. You will ensure that all information you provide to us via the AWS Site (e.g., information provided in connection with your registration for the Services, requests for increased usage limits) is accurate, complete, and not misleading.

1.6. From time to time, we may apply upgrades, patches, bug fixes, or other maintenance to the Services and AWS Content ("Maintenance"). We agree to use reasonable efforts to provide you with prior notice of any scheduled Maintenance (except for emergency Maintenance), and you agree to use reasonable efforts to comply with any Maintenance requirements that we notify you about.

1.7. If your Agreement does not include a provision on AWS Confidential Information, and you and AWS do not have an effective non-disclosure agreement in place, then you agree that you will not disclose AWS Confidential Information (as defined in the AWS Customer Agreement), except as required by law.

1.8. You may perform benchmarks or comparative tests or evaluations (each, a "Benchmark") of the Services. If you perform or disclose, or direct or permit any third party to perform or disclose, any Benchmark of any of the Services, you (i) will include in any disclosure, and will disclose to us, all information necessary to replicate such Benchmark, and (ii) agree that we may perform and disclose the results of Benchmarks of your products or services, irrespective of any restrictions on Benchmarks in the terms governing your products or services.

1.9. Only the applicable AWS Contracting Party (as defined in the AWS Customer Agreement) will have obligations with respect to each AWS account, and no other AWS Contracting Party has any obligation with respect to such account. The AWS Contracting Party for an account may change as described in the Agreement, and the new AWS Contracting Party will be responsible for issuing any invoices to you after such change, including monthly invoices. Invoices for each account will reflect the AWS Contracting Party that is responsible for that account during the applicable billing period. You agree to accept invoices from AWS electronically, in a format and method of delivery as determined by AWS, e.g., in a PDF format, as permitted under applicable law.

If, as of the time of a change of the AWS Contracting Party responsible for your account, you have made an up-front payment for any Services under such account, then the AWS Contracting Party you paid such up-front payment to may remain the AWS Contracting Party for the applicable account only with respect to the Services related to such up-front payment.

1.10. When you use a Service, you may be able to use or be required to use one or more other Services (each, an "Associated Service"), and when you use an Associated Service, you are subject to the terms and fees that apply to that Associated Service.

1.11. If you process the personal data of End Users or other identifiable individuals in your use of a Service, you are responsible for providing legally adequate privacy notices and obtaining necessary consents for the processing of such data. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for processing such data in accordance with applicable law.

1.12. If you have been charged for a Service for a period when that Service was unavailable (as defined in the applicable Service Level Agreement for each Service), you may request a Service credit equal to any charged amounts for such period.

1.13. If you are a customer that is subject to the French Politique générale de sécurité des systems d'information de santé (PGSSI-S), you agree that your use of the Services complies with the PGSSI-S.

1.14. Data Protection.

1.14.1 These Service Terms incorporate the AWS Data Processing Addendum ("DPA"), when you use AWS Services to process Customer Data (as defined in the DPA).

1.14.2 These Service Terms incorporate the AWS Supplementary Addendum to the DPA, when you use AWS Services to process Customer Data (as defined in the DPA).

1.14.3 These Service Terms incorporate the Standard Contractual Clauses between controllers and processors ("Controller-to-Processor Clauses") and the Standard Contractual Clauses between processors ("Processor-to-Processor Clauses") approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "SCCs"). The SCCs will only apply when: (i) the GDPR applies to your use of the AWS Services to process Customer Data; and (ii) Customer Data is transferred either directly or via onward transfer, to a country outside of the European Economic Area not recognised by the European Commission as providing an adequate level of protection for personal data subject to GDPR (together a "Data Transfer"). When you are a controller (as defined in the GDPR), the Controller-to-Processor Clauses will apply to a Data Transfer. When you are a processor (as defined in the GDPR), the Processor-to-Processor Clauses will apply to a Data Transfer.

1.14.4 These Service Terms incorporate the AWS UK GDPR Addendum to the DPA, when the UK GDPR applies to your use of the AWS Services to process UK Customer Data (as defined in the AWS UK GDPR Addendum), and the AWS Swiss Addendum to the DPA, when the FDPA applies to your use of the AWS Services to process Swiss Customer Data (as defined in the AWS Swiss Addendum).

1.14.5 These Service Terms incorporate the AWS CCPA Terms ("CCPA Terms"), when the CCPA applies to your use of the AWS Services to process Personal Information (as defined in the CCPA Terms).

1.15. Following closure of your AWS account, we will delete Your Content in accordance with the technical documentation applicable to the Services.

1.16. Your receipt and use of any Promotional Credits is subject to the AWS Promotional Credit Terms & Conditions.

1.17. Payment Currency

1.17.1 AWS provides a Service that enables payment in certain currencies ("Payment Currency") other than United States dollars when you purchase certain Services from AWS (the "Currency Service"). When you purchase Services in certain countries outside of the United States, we may require you, because of currency controls or other factors, to use the Currency Service. When using the Currency Service you are not tendering payment in one currency and receiving from us another currency.

1.17.2 When you use the Currency Service, Service fees and charges will automatically be invoiced in the Payment Currency. You must pay invoices in the currency specified on each invoice, but, for credit card or debit card purchases, you may only make payments in currencies supported by the issuer of your card. If the issuer of your credit card or debit card does not support the required Payment Currency, you must use a different payment method that does support paying in the Payment Currency.

1.17.3 Our fees and charges for your use of the Currency Service, if any, are included in the exchange rate applied to your invoice (the "Applicable Exchange Rate"). Third-parties, such as your bank, credit card issuer, debit card issuer, or card network, may charge you additional fees. The Applicable Exchange Rate is determined at the time your invoice is generated and, for invoices covering usage of Services over a period of time, will apply to all usage and Service charges listed on that invoice.

1.17.4 All refunds processed against an invoice will be provided in the currency in which the invoice was generated and reflected as a credit memo or a payment in your Payment Currency.

1.17.5 You agree that by using the Currency Service, information related to your payment, including your name and address, may be used by our banking partners to process your payments in jurisdictions other than the United States.

1.18. By accessing and using AWS Content or the Services, you agree to the terms of the Intellectual Property License.

1.19. We will not use Individualized Usage Data or Your Content to compete with your products and services. "Individualized Usage Data" means data about your use of the Services that are specifically identified with your AWS account.

1.20. We may use information about how you use and interact with the Services to improve those Services.

1.21. Information included in resource identifiers, metadata tags, access controls, rules, usage policies, permissions, and similar items related to the management of AWS resources does not constitute Your Content. AWS recommends that you do not include personally identifying, confidential, or sensitive information in these items.

1.22. Tax Exempt Status

1.22.1 To request tax exempt status for your AWS account, you must provide us with a valid tax exemption certificate or other equivalent documentation for the relevant jurisdiction. You are responsible for updating such documentation so it is accurate at all times.

1.22.2 In certain jurisdictions (as noted in the AWS Tax Help pages), you may only use your tax-exempt account to purchase services that are eligible for tax exemption. If you do not use services for the purpose for which your tax exemption applies, you are responsible for reporting and paying sales and use taxes for that usage directly to the relevant tax authorities to the extent required by law.

1.22.3 If you are required by law to pay us using your organization's funds to qualify for your tax exemption, you warrant that purchases on your account will be made with the tax-exempt organization's funds.

1.22.4 We may, in our sole discretion, reject your request for tax exempt status or revoke the tax exempt status of your account at any time.

1.22.5 If you turn on tax settings inheritance, you warrant that the application of any tax exemption on your Management Account to your Organization's Member Accounts (both as defined in the AWS Organizations section below) complies with applicable tax laws. If a governmental authority determines that the correct amount of tax has not been collected on your purchases, you will promptly reimburse AWS for any associated costs.

1.23. If you use any artificial intelligence and machine learning Services, features, and functionality (including third-party models) that we provide, you will comply with the AWS Responsible AI Policy.

1.24. Certain Services may incorporate generative AI features, powered by Amazon Bedrock, that enable you to use prompts to generate output, including: Amazon CloudWatch, Amazon CodeCatalyst, Amazon Connect Contact Lens, Amazon DataZone, Amazon Lex, Amazon Personalize, Amazon Q, AWS AppFabric, AWS HealthScribe, and AWS App Studio. The Amazon Bedrock automated abuse detection mechanisms may apply to such services. See here for more details.

1.25. You will not use, and will not facilitate or allow End Users to use, the Services to mine cryptocurrency without our prior written approval.

1.26. AWS consents to the assignment of an AWS account from one entity to another, subject to the terms of the AWS Account Assignment Requirements, posted here.

1.27. To benefit from any contract with AWS enabling you to use AWS Services under the same terms as your affiliate's Agreement solely because your accounts are joined as Member Accounts of their Organization (as defined in the AWS Organizations section below), your AWS Contracting Party must be a signatory to your affiliate's Agreement.

2. Betas and Previews

2.1. This Section describes the additional terms and conditions under which you may (a) access and use certain features, technologies, and services made available to you by AWS that are not yet generally available, including, but not limited to, any products, services, or features labeled “beta”, “preview”, “pre-release”, or “experimental”, and any related AWS Content (each, a “Beta Service”) or (b) access and use Services and any related AWS Content available in AWS regions that are not generally available, including, but not limited to, any AWS regions identified by AWS as “beta”, “preview”, “pre-release”, or “experimental” (each, a “Beta Region”).

2.2. You must comply with all terms related to any Beta Service or Beta Region as posted on the AWS Site or otherwise made available to you. AWS may add or modify terms, including lowering or raising any usage limits, related to access to or use of any Beta Services or Beta Regions at any time. AWS may add, modify, or remove functionality, features, documentation, or other related aspects of any Beta Service or Beta Region at any time and these aspects may be different from any generally available version of the applicable Beta Service or Beta Region. Service Level Agreements do not apply to Beta Services or Beta Regions.

2.3. You may provide AWS with information relating to your access, use, testing, or evaluation of Beta Services or Beta Regions, including observations or information regarding the performance, features, and functionality of Beta Services or Beta Regions (“Test Observations”). AWS will own and may use and evaluate all Test Observations for its own purposes. You will not use any Test Observations except for your internal evaluation purposes of any Beta Service or Beta Region.

2.4. AWS may suspend or terminate your access to or use of any Beta Service or Beta Region at any time. Your access to and use of each Beta Service and Beta Region will automatically terminate upon the release of a generally available version of the applicable Beta Service or Beta Region or upon notice of termination by AWS. Unless otherwise communicated to You, any Beta Service or Beta Region made available to You is provided for evaluation purposes and should not be used for processing sensitive data. Notwithstanding anything to the contrary in the Agreement, after suspension or termination of your access to or use of any Beta Service or Beta Region for any reason, (a) you will not have any further right to access or use the applicable Beta Service or Beta Region, and (b) Your Content used in the applicable Beta Service or Beta Region may be deleted or inaccessible and Your Content may not be migrated over to a generally available version of the applicable Beta Service or Beta Region.

2.5. Test Observations, Suggestions concerning a Beta Service or Beta Region, and any other information about or involving (including the existence of) any Beta Service or Beta Region are considered AWS Confidential Information.

2.6. WITHOUT LIMITING ANY DISCLAIMERS IN THE AGREEMENT OR THE SERVICE TERMS, BETA SERVICES AND BETA REGIONS ARE NOT READY FOR GENERAL COMMERCIAL RELEASE AND MAY CONTAIN BUGS, ERRORS, DEFECTS, OR HARMFUL COMPONENTS. ACCORDINGLY, AND NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT OR THESE SERVICES TERMS, AWS IS PROVIDING BETA SERVICES AND BETA REGIONS TO YOU "AS IS." AWS AND ITS AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE REGARDING BETA SERVICES AND BETA REGIONS, INCLUDING ANY WARRANTY THAT THE BETA SERVICES AND BETA REGIONS WILL BECOME GENERALLY AVAILABLE, BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, AWS AND ITS AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE. AWS'S AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY FOR ANY BETA SERVICES AND BETA REGIONS WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE BETA SERVICES OR BETA REGIONS THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

3. Amazon CloudFront

You must own or have all necessary rights to use any domain name or SSL certificate that you use in conjunction with Amazon CloudFront. You are solely responsible for the renewal, security, and proper configuration of any SSL certificates that you provide for use with Amazon CloudFront, including any disclosure of your SSL certificates to third parties.

4. AWS Outposts

4.1. "AWS Outposts" includes AWS Outposts racks and AWS Outposts servers.

4.2. Outposts Equipment. AWS will make equipment available to you to support your use of the AWS Outposts Service (the "Outposts Equipment"). AWS or its affiliates maintain all rights in the Outposts Equipment and is not selling, renting, leasing, or transferring any ownership, intellectual or other rights in the Outposts Equipment to you. You will not, and will not purport to, assign, grant, or transfer the Outposts Equipment or any interest in the Outposts Equipment to any individual or entity, and any such purported assignment, grant or transfer is void.

4.3. Facility Assessment. You will ensure that, at all times, the facility at which the Outposts Equipment is located (the "Designated Facility") meets the minimum requirements necessary to support the installation, maintenance, use, and removal of the Outposts Equipment as described here and otherwise as described in the Outposts technical documentation or indicated to you during the ordering and installation process.

4.4. Delivery and Use. You will ensure that you have all necessary rights, certifications, and licenses for the delivery, installation, maintenance, use, and removal of the Outposts Equipment at the Designated Facility. You are responsible for any damage to the Outposts Equipment while it is at the Designated Facility, unless caused by AWS. AWS may terminate your use of AWS Outposts and remove the Outposts Equipment if you breach these terms or materially breach the terms of the Agreement with respect to AWS Outposts. In the event that we terminate your use of AWS Outposts and remove the Outposts Equipment in accordance with this Section 4.4, we will provide you with prior notice where practicable under the circumstances.

4.5. Access to Outposts Equipment. You will give personnel designated by AWS prompt and reasonable access to the Designated Facility as necessary to deliver, install, inspect, maintain, and remove the Outposts Equipment. You will not require AWS personnel to sign, accept, or otherwise agree to any documentation as a condition of accessing the Designated Facility, and you agree that the terms of any such documentation are void even if signed by AWS personnel. You will ensure that no one accesses, moves, or repairs the Outposts Equipment other than (i) personnel designated by AWS, (ii) as permitted in writing by AWS in connection with the maintenance of Outposts Equipment, or (iii) as necessary due to a situation involving imminent injury, damage to property, or an active fire alarm system. You will ensure that no one modifies, alters, reverse engineers, or tampers with the Outposts Equipment. You acknowledge that the Outposts Equipment may be equipped with tamper monitoring.

4.6. AWS Support Options. You will remain enrolled in either Enterprise On-Ramp Support or Enterprise Support during the entire period of your use of AWS Outposts.

4.7. Services/SLAs/Security. The Service Terms for any Services that run locally on AWS Outposts also apply to your use of those Services on AWS Outposts. There are inherent differences between Services running locally on AWS Outposts from those Services running at AWS operated facilities because the Outposts Equipment is physically located at the Designated Facility where you are responsible for physical security and access controls, as well as all power, networking, and environmental conditions. Due to these differences:

a. The Service Level Agreements for any Services that run locally on AWS Outposts do not apply to your use of those Services on AWS Outposts.

b. Any AWS commitments in the Agreement that depend on AWS's operation of such physical security and access controls, or power, networking, and environmental conditions, do not apply to AWS Outposts or any Services running locally on AWS Outposts.

c. The specific compliance and assurance programs for which AWS Outposts are in scope are listed here. For other Services listed here, those Services are not in scope when running locally on AWS Outposts unless AWS Outposts is also separately listed for the specific compliance or assurance program.

4.8. AWS Outposts servers

4.8.1. Installation, Use, and Removal. You are responsible for the installation, use, and removal of the AWS Outposts servers at the Designated Facility and returning the Outposts Equipment to AWS as described in the Outposts technical documentation or as otherwise indicated to you during the ordering process. In addition to other rights and remedies AWS may have under the Agreement, AWS may charge you a lost device fee if the Outposts Equipment is lost between when it is first in your possession and when the carrier accepts the Outposts Equipment for delivery back to AWS. You must notify and obtain AWS's consent before moving the Outpost Equipment from the Designated Facility.

5. Amazon Elastic Compute Cloud

5.1. In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the "Microsoft Software").

5.1.1. If you use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

- The Microsoft Software is neither sold nor distributed to you, and you may use it solely in conjunction with the Services.
- You may not transfer or use the Microsoft Software outside the Services.
- You may not remove, modify, or obscure any copyright, trademark, or other proprietary rights notices that are contained in or on the Microsoft Software.
- You may not reverse engineer, decompile, or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.
- Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.

- You are not granted any right to use the Microsoft Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, "High Risk Use"). Microsoft and its suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.
- Microsoft is an intended third-party beneficiary of this Section 5.1.1, with the right to enforce its provisions.

5.1.2. For any instance running Microsoft Software (each, a "Microsoft Instance"), you may not use nesting, container, or similar technologies to sell or resell multiple instances, portions of an instance, or containers running within the Microsoft Instance, unless (a) you are the ultimate end user of the Microsoft Instance, (b) you have supplemented the Microsoft Instance with your own applications, or (c) you have added primary and significant functionality to the Microsoft Instance.

5.2. In conjunction with the Services, you may be allowed to use certain software (including related support, maintenance, and documentation) developed, owned, or provided by third parties or their licensors. Use of third party software is subject to these additional terms and conditions:

- Your use of NVIDIA Corporation's GRID Software is subject to the terms and conditions of the NVIDIA GRID Cloud End User License Agreement.
- Your use of NVIDIA Corporation's Tesla Driver, CUDA Toolkit, cuDNN, NVENC, NVCUVID, NVM:, nvidia-smi, and NCCL Library Software, toolkits, and drivers is subject to the terms and conditions of the NVIDIA Cloud End User License Agreement and NVIDIA Third Party Materials Notices.
- Your use of Red Hat, Inc.'s software is subject to the terms and conditions of the Red Hat Cloud Software Subscription Agreement. Red Hat also disclaims any (i) warranties with respect to Red Hat, Inc. software; and (ii) liability for any damages, whether direct, indirect, incidental, special, punitive or consequential, and any loss of profits, revenue, data or data use, arising from use of Red Hat, Inc. software.
- Your use of SUSE LLC's software is subject to the terms and conditions of the SUSE End User License Agreement and the SUSE Terms and Conditions.
- Your use of Apple Inc.'s software is subject to the terms and conditions of the applicable Apple Software License Agreement.
- Your use of Qualcomm Technologies Inc.'s software is subject to the terms and conditions of Qualcomm's Software Development Kit License Agreement.

5.3. Unless you specify a termination date, your Spot Instance request will remain active until the earlier of the following: (1) seven days have passed, (2) we fulfill it, or (3) you cancel it. We may terminate, stop, or hibernate Spot Instances at any time and without any notice to you if the current price for the applicable Spot Instance (the "Spot Price") equals or exceeds the price you specified you were willing to pay for the Spot Instance ("Your Maximum Price"). Spot Instances purchased for a fixed duration ("Spot Blocks") will not be terminated because the Spot Price equals or exceeds Your Maximum Price (if specified), but

will terminate at the conclusion of the fixed duration. Spot Instances and Spot Blocks may also be terminated for AWS capacity requirements. If a Spot Block is terminated due to AWS capacity requirements, you will not be charged for that Spot Block. Spot Instances may not be used with certain Services, features, and third-party software we specify, including IBM software packages or Microsoft SQL Server. You may not, directly, indirectly, alone, or in cooperation with any third party, attempt to control, influence, or manipulate the price for Spot Instances. You may not submit requests for Spot Instances through any third party (e.g., "proxy bidding") or share information with any third party regarding Your Maximum Price specified in your Spot Instance Requests.

5.4. EC2 Reserved Instances and Dedicated Hosts.

5.4.1. We may change Savings Plans, EC2 Reserved Instance and EC2 Dedicated Host Reservation pricing at any time, but price changes will not apply to previously designated Savings Plans, EC2 Reserved Instances or EC2 Dedicated Host Reservations, except as described in this Section 5.4. If Microsoft increases the license fees it charges for Windows, or if Red Hat increases the license fees it charges for Red Hat Enterprise Linux ("RHEL"), we may make a corresponding increase to the per-hour usage rate (or institute a corresponding per-hour usage rate) for Savings Plans for, or EC2 Reserved Instances with, Windows or RHEL. Any increase in (or institution of) the per-hour usage rate for Savings Plans for, or EC2 Reserved Instances with, Windows will be made between December 1 and January 31, and we will provide 30 days' notice. For any increase in (or institution of) the per-hour usage rate for Savings Plans for, or EC2 Reserved Instances with, RHEL, we will provide 30 days' advance notice. If this happens, you may: (a) continue to use your EC2 Reserved Instances with Windows or RHEL with the new per-hour usage price; (b) convert your EC2 Reserved Instances with Windows or RHEL to comparable EC2 Reserved Instances with Linux; or (c) terminate your EC2 Reserved Instances with Windows or RHEL and receive a pro rata refund of the up-front fee you paid for the terminated EC2 Reserved Instances with Windows or RHEL.

5.4.2. We may terminate the Savings Plans, EC2 Reserved Instance or EC2 Dedicated Host Reservation pricing programs at any time. Savings Plans and EC2 Dedicated Hosts are nontransferable, and EC2 Reserved Instances are only transferrable in accordance with the requirements of the RI Marketplace provided on the AWS Site. Scheduled Instances and Convertible Reserved Instances are not eligible for the RI Marketplace. Savings Plans, EC2 Reserved Instances and EC2 Dedicated Host Reservations are noncancellable, and EC2 Dedicated Hosts associated with an active EC2 Dedicated Host Reservation cannot be removed from your account, so you will be charged for the duration of the term you selected, even if you terminate the Agreement. All amounts paid in connection with Savings Plans, EC2 Reserved Instances and EC2 Dedicated Host Reservations are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual EC2 Reserved Instance or EC2 Dedicated Host Reservation type, or terminate the Savings Plans, EC2 Reserved Instance or EC2 Dedicated Host pricing program(s), we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Savings Plans, EC2 Reserved Instances or EC2 Dedicated Hosts. You may not purchase EC2 Reserved Instances for the purpose of reselling them in the RI Marketplace, and we reserve the right to refuse or cancel your purchase if we suspect you are doing so. Upon expiration or termination of the term of Savings Plans, EC2 Reserved Instances or EC2 Dedicated Host Reservations, the reserved pricing will expire and standard on-demand usage prices will apply. You are responsible for determining if you are subject to any limitations arising from the purchase or Savings Plans, EC2 Reserved Instances or EC2 Dedicated Host Reservations. For

example, you are responsible for complying with any applicable laws, policies, terms or conditions governing your payment of up-front fees or the expiration of reserved resources, including any fiscal or appropriation laws, or other policies or restrictions governing up-front payments for goods or services.

5.5. EC2 Capacity Blocks for ML. AWS Capacity Blocks cannot be canceled nor can they be modified, and the full price of a Capacity Block is nonrefundable. You are responsible for determining if you are subject to any limitations arising from the purchase of Capacity Blocks. For example, you are responsible for complying with any applicable laws, policies, terms or conditions governing your payment of up-front fees or the expiration of reserved resources, including any fiscal or appropriation laws, or other policies or restrictions governing up-front payments for goods or services. During the final 30 minutes of a Capacity Block, we may terminate your instances without notice and prevent new instance launches into your reservation. Capacity Blocks are nontransferable. Capacity Blocks that you purchase cannot be resold to another party, and we reserve the right to refuse or cancel your purchase if we suspect you are doing so. You may not cooperate with any third party in an attempt to influence or manipulate the price for Capacity Blocks. You may not submit requests for Capacity Blocks through any third party (e.g., "proxy purchasing").

5.6. EC2 Reserved Instance (RI) Marketplace.

5.6.1. The rights to an active EC2 Reserved Instance can be offered for sale through the RI Marketplace as long as (1) the remaining term on the Reserved Instance is greater than 1 month and (2) your payment of the upfront charge for it has been received and processed (for credit card purchases, 30 days after you have paid the upfront fee, and for invoice purchases, after you have paid the applicable invoice) (a "Marketable EC2 Reserved Instance"). You can be a "Seller" if you are a current AWS customer in good standing, you have a Marketable EC2 Reserved Instance associated with your AWS account, and you complete the registration process through your AWS account. You can be a "Buyer" if you are a current AWS customer in good standing. Non-U.S.-based entities may not be Sellers without providing the Form W-8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding) to establish that you are not a U.S. person. You can resell an EC2 Reserved Instance that you previously purchased through the RI Marketplace. You may not resell an EC2 Reserved Instance that you purchased through a discount program (Reserved Instance Volume Discounts or otherwise) without obtaining our prior approval.

5.6.2. As a Seller, you will be the seller of record of your rights to a Marketable EC2 Reserved Instance. Except as expressly set forth in these Service Terms, we are not involved in any underlying transaction between you and any Buyer. We or our affiliates may also participate in the RI Marketplace as a Seller or a Buyer. We may remove any Marketable EC2 Reserved Instance from the RI Marketplace at any time. Once sold and transferred to a Buyer, a Seller will have no rights to that Marketable EC2 Reserved Instance.

5.6.3. On Seller's behalf, we will process all payments for Transactions and collect the applicable Transaction Proceeds. "Transaction" means any sale of a Marketable EC2 Reserved Instance through the RI Marketplace. "Transaction Proceeds" means the gross sales proceeds received by us from any Transaction. You will ensure that all fees and charges payable by Buyers for Marketable EC2 Reserved Instance are billed and collected through us and you will not offer or

establish any alternative means of payment. We may impose transaction limits on some or all Buyers and Sellers relating to the value of any Transaction or disbursement, the cumulative value of all Transactions or disbursements during a period of time, or the number of Transactions that we will process over a period of time. We may withhold for investigation, or refuse to process, any Transaction that we suspect is fraudulent, unlawful, or otherwise violates these Service Terms, the Agreement, or the Acceptable Use Policy. For each Transaction, we will not remit Transaction Proceeds to a Seller, and the Marketable EC2 Reserved Instance will not be available to the Buyer, until after we have successfully processed payments for that Transaction from the Buyer.

5.6.4. You will not receive any funds collected from payments associated with the hourly prices of your Marketable EC2 Reserved Instance. At the end of each business day, we will pay to you all due and payable Transaction Proceeds that we have collected as of the date that is 2 business days prior to that date. We will deduct from each payment any applicable fees and charges due to us related to Marketable EC2 Reserved Instances. We may withhold, deduct, or setoff any amounts payable by you to us or our affiliates against any Transaction Proceeds. Payments will be made only to an ACH-enabled bank account located in the United States that you register with us. If there is an error in the processing of any Transaction, you authorize us to initiate debit or credit entries to your designated bank account, to correct such error, provided that any such correction is made in accordance with applicable laws and regulations. If we are unable to debit your designated bank account for any reason, you authorize us to resubmit the debit, plus any applicable fees, to any other bank account or payment instrument that you have on file with us or to deduct the debit and applicable fees from future Transaction Proceeds.

5.6.5. Sellers are responsible for the calculation, validation, and payment of any and all sales, use, excise, import, export, value added, withholding, and other taxes and duties assessed, incurred, or required to be collected or paid ("Taxes") for any reason in connection with any Transaction and with any Marketable EC2 Reserved Instance. We are not responsible for determining whether any Taxes apply to any Transaction or remitting Taxes to any taxing authority with respect to any Transaction, or for reporting any information (including the payment of Taxes) with respect to any Transaction. Each Seller will indemnify us and our affiliates against any claim or demand for payment of any Taxes imposed in connection with any Transaction, and for any fines, penalties, or similar charges imposed as a result of the Seller's failure to collect, remit, or report any Taxes in connection with any Transaction.

5.6.6. For each Seller, we will collect the necessary data and tax forms to enable compliance with applicable tax laws. For example, for U.S.-based Sellers, we will collect and retain Seller name and address, and may collect the tax identification number and other data as needed to comply with Form 1099K reporting requirements; for non-U.S.-based Sellers, we will collect and retain a Form W-8BEN tax form (which includes name, address, and a signature) as proof that you are exempt from Form 1099K reporting. For each Buyer, we will collect and retain the Buyer's name and address. Buyers and Sellers will not know the name of the other party to the Transaction until the Transaction is completed. Upon completion of the Transaction, we will share the applicable Buyer's city, state, and zip with the Seller so that the Seller can calculate the appropriate tax (if any) to remit to the appropriate government entity. We will share the Seller's legal name on the Buyer's invoice. Buyers and Sellers may not use information about the Transaction or about the other party gained in connection with a Transaction ("Transaction Information") for any purpose that is not related to the Transaction. For example, you may not, directly or indirectly: (1) disclose any Transaction Information to any third party, except as necessary for you to perform your tax obligations or other obligations under these Service Terms and only if you ensure that every recipient uses the information only for that purpose and complies with these restrictions; (2) use any Transaction Information for any

marketing or promotional purposes whatsoever; (3) use any Transaction Information in any way inconsistent with applicable law; (4) contact a party to influence them to make an alternative sale or purchase; or (5) target communications of any kind on the basis of the intended recipient being an RI Marketplace Buyer or Seller.

5.7. Amazon EC2 enables you to provision Amazon EC2 instances using your Microsoft Software and Microsoft Licenses (the "BYOL Program"). Unless otherwise specified in your agreement(s) with Microsoft, you can participate in the BYOL Program only if you comply with the requirements here, and you (a) use Dedicated Instances or Dedicated Hosts; and (b) launch from Virtual Machines (VMs) sourced from software binaries provided by you.

You must be eligible to use the BYOL Program for the applicable Microsoft Software under your agreements with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. By using the Microsoft Software under the BYOL Program, you agree to Microsoft's End User License Agreement.

You agree that you have determined that your use of the BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted.

5.8. As part of using Amazon EC2, you agree that your Amazon EC2 resources may be terminated or replaced due to failure, retirement or other AWS requirements. THE USE OF AMAZON EC2 DOES NOT GRANT YOU, AND YOU HEREBY WAIVE, ANY RIGHT OF PHYSICAL ACCESS TO, OR PHYSICAL POSSESSION OF, ANY AWS SERVERS, EQUIPMENT, REAL OR PERSONAL PROPERTY, OR OTHER ASSETS.

6. Alexa Web Services

You may use data you receive from the Alexa Services Web Information Service and Alexa Top Sites (collectively "Alexa Web Services"), such as web site traffic data, to enhance your application or website, but may not use it in any application whose primary purpose is to display the same or related data or to compete with www.alexa.com. You may not display data you receive via the Alexa Web Services that has been cached for more than 24 hours. You may not resell or redistribute the Alexa Web Services or data you access via the Alexa Web Services.

7. Amazon SimpleDB Service (Amazon SimpleDB)

If during the previous 6 months you have incurred no fees for Amazon SimpleDB and have registered no usage of Your Content stored in Amazon SimpleDB, we may delete Your Content that is stored in Simple DB upon 30 days prior notice to you.

8. Amazon CloudWatch and Autoscaling

8.1. Amazon CloudWatch collects and stores certain information for the Services you are monitoring, including CPU utilization, data transfer, and disk usage and activity (collectively, “CloudWatch Metric Data”). CloudWatch Metric Data may be used by AWS to develop and improve the Services.

8.2. You agree and instruct that when using any Amazon CloudWatch ML Functionality, (a) we may use and store your Amazon CloudWatch ML Content to develop and improve that functionality and its underlying technologies and (b) solely in connection with the development and improvement described in clause (a), we may use your Amazon CloudWatch ML Content in an AWS region outside of the AWS region where you are using Amazon CloudWatch. You may instruct AWS not to use and store your Amazon CloudWatch ML Content as described in the prior sentence by configuring an AI services opt-out policy using AWS Organizations. “Amazon CloudWatch ML Functionality” means any Amazon CloudWatch functionalities identified to you as powered by artificial intelligence or machine learning. “Amazon CloudWatch ML Content” means Your Content that is processed by an Amazon CloudWatch ML Functionality. In addition, the Amazon CloudWatch ML Functionality entitled “query builder” may be used solely for purposes of building a query for your metrics or logs.

8.3. Amazon CloudWatch Network Monitoring

8.3.1. “Amazon CloudWatch Network Monitoring” includes Amazon CloudWatch Internet Monitor and Amazon CloudWatch Network Monitor.

8.3.2. This Section applies to data provided by monitors in your AWS account and in third party AWS accounts. You may not, and may not allow any third party to, use Amazon CloudWatch Network Monitoring, or any data or information made available through Amazon CloudWatch Network Monitoring, to, directly or indirectly, develop, improve, or offer a similar or competing product or service. You may not resell or redistribute Amazon CloudWatch Network Monitoring or any metrics provided by Amazon CloudWatch Network Monitoring unless you have been authorized as an AWS reseller, you add material value as part of the resale or redistribution, you restrict recipients from further reselling or redistributing to any additional entities, and for each monitor, you do not resell or redistribute metrics provided by the monitor to more than one entity. You may distribute metrics provided by your monitor(s) to third party network observability services solely for your personal use.

9. AWS Snowball and AWS Snowcone

9.1. “AWS Snow Family” includes: AWS Snowball and AWS Snowcone.

9.2. As part of AWS Snowball and AWS Snowcone, we will ship you an agreed upon number of “Snowball” or "Snowcone" hardware appliances (each an “Appliance”) and provide you with access to the applicable AWS Snowball Client or AWS Snowcone client software (together with the software contained on the Appliance, and any updates or upgrades to the foregoing, the “Appliance Software”). You agree that you will not allow any Appliance to leave the country to which the Appliance is shipped until you provide it (in the same country) to a carrier for redelivery to us. Upon our request for any reason, you will promptly return any appliance to us. Appliances collect and provide us with metrics regarding the use of Appliances, including boot times, size of transferred files,

duration of transfers, and errors or timeouts. These metrics may be associated with your account ID, and we may use these metrics to maintain, provide, develop, and improve the Services.

9.3. Once AWS Snow Family services are complete, we will delete data from the Appliances.

9.4. You are responsible for payment of all customs, duties, taxes, and other charges in connection with Appliances being shipped to or from us.

9.5. You are responsible for any damage to, or loss of, an Appliance after delivery to you until the carrier accepts the Appliance for delivery back to us. In addition to other rights and remedies we may have under the Agreement, we may charge you the applicable lost device fee specified on the AWS Snowball or AWS Snowcone pricing pages if: (a) an Appliance is lost or irreparably damaged between when it is first in your possession and when the carrier accepts the Appliance for delivery back to us; or (b) you do not provide the Appliance to the carrier for return to us at our request.

9.6. YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA AND YOUR USE OF APPLIANCES , INCLUDING ENCRYPTING SENSITIVE DATA AND NOT ALLOWING UNAUTHORIZED ACCESS TO ANY APPLIANCE.

9.7. AWS or its affiliates maintain all rights in the Appliances and Appliance Software, and is not selling, renting, leasing, or transferring any ownership, intellectual or other rights in the Appliances or Appliance Software to you. You will not, and will not purport to, assign, grant, or transfer the Appliances or Appliance Software or any interest in the Appliances or Appliance Software to any individual or entity, and any such purported assignment, grant or transfer is void. Without limiting the foregoing, you will not (or attempt to), and will not permit or authorize third parties to (or attempt to), (a) scan, x-ray, open, modify, alter, disassemble, or otherwise attempt to view the inside of or tamper with the Appliance; or (b) circumvent or disable any features or measures in the Appliance or Appliance Software. You acknowledge that the Appliances may be equipped with tamper monitoring.

9.8. You will return all Appliances to us for assessment and to enable us to determine how they can be reused and which components must be recycled in an environmentally sound manner, regardless of the external condition of the Appliance and even if you believe the Appliance may be damaged or non-functional. You will not, under any circumstance, treat or dispose of an Appliance (or any component thereof, including internal batteries) as waste. Shipments of used Appliances must be conducted in a manner consistent with applicable laws relating to used electronic equipment, including where applicable the Basel Convention Technical Guidelines on Transboundary Movement of Used Electrical and Electronic Equipment.

9.9. You are responsible for complying with all applicable data protection, import, re-import, export, and re-export control laws, including any applicable license requirements, and country-specific sanctions programs. You are responsible for serving as the exporter and importer of record (as applicable) for your data, software, or technology, and you accept that AWS will not participate in the export or import procedure. If you are using Appliances or Appliance Software for dual use items in the European Union, you represent that you, or the legal entity you represent, are “established” in the European Union; or, if you

are not “established” in the European Union, that you will not upload, request that we download, or export such dual-use items outside the European Union. If you are using Appliances or Appliance Software in the European Union for military items, you represent that you, or the legal entity you represent, are permitted by the Member State of your incorporation to upload, request that we download or export any such military items from that Member State, and it is a condition of this Agreement and your use of AWS Snow Family that you are so permitted.

10. Amazon Relational Database Service (Amazon RDS)

10.1. You may store snapshots of Your Amazon RDS Content for later use in Amazon RDS, but snapshots cannot be downloaded outside the Services.

10.2. The Reserved DB Instance program allows you to designate Amazon RDS database instances as subject to the reserved pricing and payment terms set forth on the Amazon RDS detail page on the AWS Site (each designated instance, a “Reserved DB Instance”). We may terminate the Reserved DB Instance program at any time. We may change pricing for the Reserved DB Instance program at any time, but price changes will not apply to previously designated Reserved DB Instances. Reserved DB Instances are noncancellable, and you will owe the amount charged for the Reserved DB Instance for the duration of the term you selected, even if the Agreement is terminated. Reserved DB Instances are nontransferable and all amounts paid in connection with the Reserved DB Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved DB Instance type, or terminate the Reserved DB Instance program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved DB Instances. Upon expiration or termination of the term of a Reserved DB Instance, the Reserved DB Instance pricing will expire and standard on-demand usage prices will apply to the database instance.

10.3. Using Oracle Software.

10.3.1. “License Included”. As part of the Services, you may be allowed to use certain software (including related documentation) described on the AWS Site developed and owned by Oracle America, Inc. or its affiliates (“Oracle”) and Oracle’s licensors (collectively, the “Oracle Software”). If you choose to use the Oracle Software and do not already have a license from Oracle for that Oracle Software, Oracle and its licensors require that you agree to these additional terms and conditions:

- Oracle or its licensors retains all ownership and intellectual property rights in the Oracle Software, and title to the Oracle Software does not transfer to you or any third party by virtue of this Agreement.
- The Oracle Software is subject to a restricted license and may only be used in connection with the Services, and only by the individual or legal entity that entered into the Agreement.

- You may only use the Oracle Software for your internal business operations and in accordance with the Agreement. You may permit agents or contractors (including outsourcers) to use the Oracle Software on your behalf for the purposes set forth in, and subject to, the Agreement, provided you are responsible for the agent's, contractor's and outsourcer's compliance with the Agreement in connection with such use.
- You may not:
    - assign, grant, or transfer the Oracle Software or any interest in the Oracle Software to another individual or entity, and if you purport to grant a security interest in the Oracle Software, the secured party will have no right to use or transfer the Oracle Software;
    - use the Oracle Software for rental, timesharing, subscription services, hosting, or outsourcing;
    - remove or modify any notice of Oracle's or its licensors' proprietary rights;
    - make the Oracle Software available in any manner to any third party for use in the third party's business operations;
    - duplicate, reverse engineer (unless required by law for interoperability), disassemble or decompile the Oracle Software (including by reviewing data structures or similar materials produced by the Oracle Software); or
    - publish any results of benchmark tests run on the Oracle Software.
- Third party technology that may be appropriate or necessary for use with some Oracle Software is specified in the related documentation, and that third party technology is licensed to you only for use with the Services and under the terms of the third party license agreement specified in the documentation, not this Agreement.
- To the extent permitted by applicable law, Oracle disclaims any liability for any damages, whether direct, indirect, incidental, special, punitive or consequential, and any loss of profits, revenue, data or data use, arising from your use of the Oracle Software.
- Notwithstanding anything to the contrary elsewhere in the Agreement, Oracle is an intended third party beneficiary of the Agreement, but solely with respect to this Section 10.3.1 of these Service Terms.
- The Uniform Computer Information Transactions Act does not apply to your use of the Oracle Software.
- Upon any termination of the Agreement, you must discontinue use of the Oracle Software and any related documentation.

10.3.2. "Bring-Your-Own-License" (BYOL). Under the BYOL option, Amazon RDS enables you to provision Oracle Software to Amazon EC2 instances and use the management capabilities of Amazon RDS for the Oracle Software. You can use the Oracle Software with Amazon RDS if you meet the following conditions:

- You must have a valid license with "Software Update License & Support" for the Oracle Software you wish to run. The terms of your existing license and support agreement(s) with Oracle continue to apply to your use of the Oracle Software; and

- You must follow Oracle's current policies for licensing Oracle Database software in the cloud computing environment. The database instances using the Oracle Software with Amazon RDS reside in the Amazon EC2 environment.

10.4. Using Microsoft Software. "License Included." Use of Microsoft Software on Amazon RDS is subject to Section 5.1 above and these additional terms and conditions:

- SQL Server Web Edition may be used only to support public and Internet accessible Web pages, Web sites, Web applications, or Web services. It may not be used to support line of business applications (e.g., Customer Relationship Management, Enterprise Resource Management, and other similar applications).
- Microsoft is an intended third-party beneficiary of this Section 10.4, with the right to enforce its provisions.

10.5. Amazon RDS Custom.

10.5.1. RDS Custom enables you to provision and manage the database engine and operating system running on an Amazon EC2 instance. In conjunction with RDS Custom, you may use certain binaries, software, or similar media (including related support, maintenance, and documentation) developed, owned, or provided by third parties or their licensors. You agree that you have determined that your use of RDS Custom complies, and will continue to comply, with applicable licensing and support requirements. Usage of RDS Custom in violation of your agreement(s) with third parties is not authorized or permitted.

Your failure to maintain your database instance within the support perimeter (as specified in the documentation) may result in Service failure for which AWS is not responsible. Your customization, copies, and use of any additional software with RDS Custom is your responsibility and may result in your RDS Custom instance falling outside the support perimeter and causing Service failure for which AWS is not responsible.

10.5.2. Your use of certain database engines or operating systems (OS) software (including related documentation) made available to you for use with RDS Custom is subject to the applicable third party licensing requirements specified below:

- Use of a Linux OS version, such as those from Red Hat, Inc., SUSE LLC, and NVIDIA Corporation, on RDS Custom is subject to Section 5.2. above.
- Use of "License Included" Microsoft Software on RDS Custom is subject to Sections 5.1. and 10.4. above.

10.6. Trusted Language Extensions for PostgresSQL (Trusted Language Extensions) enables you to use, build, and run extensions developed, owned, or provided by you, third parties, or their licensors using PostgreSQL trusted languages in Amazon RDS. Extension code that you use with Trusted Language Extensions is Your Content under the Agreement. AWS is not responsible for Service failure caused by extensions. You consent to AWS scanning extension code for security and performance purposes.

10.7. Using IBM Software

10.7.1. "Bring-Your-Own-License" (BYOL). Under the BYOL option, Amazon RDS enables you to provision IBM Db2 software on Amazon RDS instances using your existing IBM Db2 software license and support entitlements obtained from IBM or an authorized IBM reseller to IBM Db2 Standard Edition or IBM Db2 Advanced Edition ("IBM Db2 Software"). You can use your existing IBM Db2 Software license under the BYOL option with Amazon RDS if you meet and agree to the following terms and conditions:

- You must have a valid license with current and ongoing "Subscription & Support" authorization from IBM or its authorized reseller for the IBM Db2 Software you wish to run. The terms and conditions of your existing license and support agreement(s) with IBM, and your compliance therewith, continue to apply to your use of IBM Db2 Software with Amazon RDS;
- You must comply with IBM's current Eligible Public Cloud Bring-Your-Own-Software-License (BYOSL) Policy including the terms associated with the IBM Db2 Software on Amazon RDS found here; and
- Your use of IBM Db2 Software with Amazon RDS is subject to suspension or termination if you do not comply with the terms and conditions above.

10.7.2. Subject to the AWS Privacy Notice (available at https://aws.amazon.com/privacy/), AWS may send information to IBM related to your IBM Db2 Software licenses such as identification numbers issued to you by IBM and the version of the IBM Db2 Software that you are using.

10.7.3. When you purchase licenses for IBM Db2 Software through the AWS Marketplace integration in the RDS console, Section 20 (AWS Marketplace) of the Service Terms apply.

11. Amazon Simple Notification Service (Amazon SNS)

11.1. Portions of Amazon SNS in Japan are sold and provided by AMCS LLC, an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

11.2 Portions of Amazon SNS in Singapore are sold and provided by AMCS SG PRIVATE LIMITED ("AMCS SG"), an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

11.3. Fees for Amazon SNS will apply regardless of whether delivery of your notifications is prevented, delayed, or blocked due to reasons outside of our control.

11.4. You are responsible for complying with legal requirements related to unsolicited or unwanted communications, including without limitation, the Telephone Consumer Protection Act (TCPA), the FTC's Telemarketing Sales Rule, and the EU e-Privacy Directive, or any other similar telemarketing law.

11.5. Amazon SNS utilizes the underlying functionality of AWS End User Messaging to send SMS messages and push notifications, and your use of Amazon SNS is also subject to the terms that govern AWS End User Messaging.

11.6. Through your use of Amazon SNS you will not:

- Transmit any material that contains viruses, Trojan horses, worms, or any other malicious or harmful programs.
- Offer or purport to offer any Emergency Services. "Emergency Services" means services that allow a user to connect with emergency services personnel or public safety answering points, such as 911 or E911 services.
- If the applicable AWS Contracting Party is AWS India, "Emergency Services" shall mean services that allow a user to connect with emergency services personnel or public safety answering points, such as 100, 112 services.
- Materially violate or facilitate the material violation of any local or foreign law, rule, regulation, or order, including laws regarding the transmission of data or software.
- Transmit material that is sexually explicit, relates to "adult services", or contains sensitive financial or identifying information (such as social security numbers)
- Resell, sublicense, or timeshare the Services, or use them on behalf of anonymous or other third parties.
- Use the Services in hazardous environments (such as operation of nuclear facilities, aircraft navigation, or any other use that may result in foreseeable risk of injury, death, or destruction of property).

12. AWS Identity and Access Management (IAM)

12.1. We may change user credentials created by you using IAM if we determine in our reasonable discretion that a change is necessary for the protection of your AWS account and resources, and we will promptly notify you of any such change.

12.2. We may change, discontinue, or deprecate support for any third-party identity provider at any time without prior notice.

13. Amazon Route 53

13.1. You may not create a hosted zone for a domain that you do not own or have authority over.

13.2. All Domain Name System (DNS) records (other than Private DNS records) used in connection with Amazon Route 53 will be publicly available, and AWS will have no liability for disclosure of those DNS records.

13.3. Domain name registration services are provided under the Amazon Route 53 Domain Name Registration Agreement.

14. AWS Elastic Beanstalk

14.1. AWS may reject or modify any URL used in connection with an AWS Elastic Beanstalk environment that violates the intellectual property rights any third-party or violates the Acceptable Use Policy.

14.2. If you stop running your AWS Elastic Beanstalk environment at any time, the [myapp] portion of the URL used in connection with the environment will no longer be available to you and may be used by another AWS customer.

15. Amazon Simple Email Service (SES)

15.1. Portions of Amazon SES in Singapore are sold and provided by AMCS SG PRIVATE LIMITED ("AMCS SG"), an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

15.2. Portions of Amazon SES in Japan are sold and provided by AMCS LLC ("AMCS"), an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

15.3. Like many email service providers, to increase the security and reliability of email you send, attempt to send, or receive using SES ("SES Email"), we (or our third-party providers) may store and scan your SES Email and Your Content included in SES Email to protect you and SES by preventing and blocking "spam" and unsolicited e-mails, "phishing" or simulated "phishing" emails, viruses and spyware, and other harmful or unwanted items from being sent and received over SES.

15.4. We may suspend or terminate your access to SES, or block or decline to send or receive any SES Email, if we determine that your use of SES fails to comply with the AWS Acceptable Use Policy and these Terms, for example if:

- our scan of SES Email or Your Content included in SES Email reveals abusive or low quality email (such as "spam" or other harmful or unwanted items),
- SES Email bounces back to us or we receive abuse complaints (including complaints from third parties) in connection with your SES Email, or

- the source or ReturnPath email address you have provided us for “address bounces” or complaints is not successfully receiving email.

15.5. If your SES Emails are blocked, delayed, or prevented from delivery by reasons outside of our control, your payment obligations continue.

15.6. AWS is not the “sender” as defined in the CAN-SPAM Act or similar applicable law.

16. AWS Direct Connect

16.1. You are responsible for protecting your AWS Direct Connect connections, including using physical security, firewalls, and other network security tools as appropriate.

16.2. AWS will permit data center operators or other service providers to connect your hardware to AWS’s hardware at the AWS Direct Connect location(s) that you select. AWS will provide the necessary information to enable the data center operator or other service provider to establish and monitor this connection, including your name, email address, network configuration, activity information, and AWS account number.

16.3. You are responsible for your separate relationship with the data center operator or other service provider, including compliance with your agreement with, and the policies and procedures of, the data center operator or other service provider, and payment of applicable fees to the data center operator or other service provider. You are responsible for providing or procuring (and AWS will not own or be responsible for) any equipment or cabling necessary to establish this dedicated connection.

16.4. If the connection you establish as part of AWS Direct Connect is temporarily unavailable or terminated, AWS will route traffic bound for your AWS resources over the public Internet and AWS’s standard data transfer charges will apply. However, if you are using Amazon Virtual Private Cloud (VPC), traffic bound for your Amazon VPC resources will be routed through an IPsec VPN connection. If an IPsec VPN connection is unavailable, traffic bound for your Amazon VPC resources will not be delivered.

17. Amazon ElastiCache

17.1. You may not access or tamper with any software we install on the cache nodes as part of Amazon ElastiCache.

17.2. The Reserved Cache Node program allows you to purchase reserved Amazon ElastiCache cache nodes subject to the reserved pricing and payment terms set forth on the Amazon ElastiCache detail page on the AWS Site (each designated instance, a “Reserved Cache Node”). We may terminate the Reserved Cache Node program at any time. We may change the pricing for Reserved Cache Nodes at any time, but price changes will not apply to previously designated

Reserved Cache Nodes. Reserved Cache Nodes are nontransferable, and all amounts paid in connection with Reserved Cache Nodes are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved Cache Node type, or terminate the Reserved Cache Node program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved Cache Nodes. Upon expiration or termination of the term of a Reserved Cache Node, standard on-demand usage prices will apply to the cache nodes you use.

18. AWS GovCloud (US) Service Terms

18.1. Use of the Services in the AWS GovCloud (US) Regions is subject to the AWS GovCloud (US) Terms and Conditions available via AWS Artifact in the AWS GovCloud (US) management console.

18.2. You are responsible for satisfying any applicable eligibility requirements for using the AWS GovCloud (US) Regions, including providing accurate and current registration information. We may make, directly or through third parties, any inquiries we consider necessary to validate information that you provide to us, including checking commercial and governmental databases. While we may take steps to verify the identity of our Customers, we cannot and do not guarantee any Customer's identity.

18.3. AWS makes no representation or warranty related to the US Persons status of any Customer or End User that may be granted access to the AWS GovCloud (US) Regions.

18.4. You are responsible for verifying the adequacy of the AWS GovCloud (US) Regions for the processing and storage of Your Content and that your use of AWS Services will comply with the laws and regulations that may govern Your Content.

19. Amazon DynamoDB

The Amazon DynamoDB Reserved Capacity program allows you to purchase reserved throughput capacity (reads and writes) subject to the pricing and payment terms set forth on the Amazon DynamoDB detail page on the AWS Site (“Amazon DynamoDB Reserved Capacity”). We may terminate the Amazon DynamoDB Reserved Capacity program at any time. We may change the pricing for Amazon DynamoDB Reserved Capacity at any time, but price changes will not apply to previously purchased Amazon DynamoDB Reserved Capacity. Amazon DynamoDB Reserved Capacity is nontransferable and all amounts paid in connection with the Amazon DynamoDB Reserved Capacity are nonrefundable, except that if we terminate the Agreement (other than for cause) or the Amazon DynamoDB Reserved Capacity program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously purchased Amazon DynamoDB Reserved Capacity. Upon expiration or termination of the term of any Amazon DynamoDB Reserved Capacity, standard on-demand usage prices will apply to your use of Amazon DynamoDB.

20. AWS Marketplace

20.1. Buyer Terms. If you purchase or obtain access to any Content or services through AWS Marketplace, the following AWS Marketplace Buyer Terms apply to you:

20.1.1. Except to the extent Content made available through AWS Marketplace is provided to you under a separate license that expressly states otherwise, neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content, (b) reverse engineer, disassemble, or decompile the Content or apply any other process or procedure to derive the source code of any software included in the Content, (c) resell or sublicense the Content, (d) transfer Content outside the Services without specific authorization to do so, or (e) tamper with or circumvent any controls or make unauthorized copies of the Content.

20.1.2. AWS may stop providing AWS Marketplace (or any features of or listings within AWS Marketplace), without prior notice to you. In addition, AWS may disable or remove Content you have purchased on AWS Marketplace, if AWS reasonably determines that the Content may violate any Policies or any other regulations, policies, or laws.

20.1.3. To the extent authorized by the respective third party provider on AWS Marketplace, AWS may disable access to or remove any Third Party Content you purchased or subscribed to on AWS Marketplace in the event of overdue and uncollected payments, upon AWS providing you with at least 30 days' advance written notice.

20.1.4. Professional services offered on AWS Marketplace by third parties are subject to separate terms and conditions specified by the respective third party. AWS has no control over and makes no guarantees about such services.

20.1.5. If you are a buyer on AWS Marketplace, you are responsible for collecting tax documentation, withholding as required, and filing all tax forms with your applicable tax authorities for your AWS Marketplace transactions. If you are a buyer making a payment of U.S. source services or royalty income to a non-U.S. third party provider, all such collection, withholding, and filing obligations are yours as we do not act as a Withholding Agent as defined by U.S. Treas. Reg. 1.1441-7(a). In certain countries, AWS will collect fees and taxes on behalf of the seller and remit the taxes and subscription payment to the seller.

20.1.6. For purposes of facilitating your purchases from third parties on AWS Marketplace, the applicable AWS Contracting Party under the Agreement is set out in the table below. Notwithstanding the foregoing, Amazon Web Services, Inc. continues to be the invoicing party for third party products that are resold by Amazon Web Services, Inc. on AWS Marketplace.

Account Country	AWS Contracting Party	Facsimile	Mailing Address
Australia (w.e.f. 1 October 2022)	Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891)	N/A	Level 37, 2-26 Park Street, Sydney, NSW, 2000, Australia
Japan (w.e.f. 1 October 2022)	Amazon Web Services Japan G.K.	N/A	1-1, Kamiosaki 3-chome, Shinagawa-ku, Tokyo, 141-0021, Japan
The countries within Europe, the Middle East, and Africa (except South Africa and Turkey) listed at[1]: https://aws.amazon.com/legal/aws-emea-countries/ (w.e.f. 1 January 2022)	Amazon Web Services EMEA SARL	352 2789 0057	38 Avenue John F. Kennedy, L-1855, Luxembourg
Any other country that is not listed in this table above	Amazon Web Services, Inc.	206-266-7010	410 Terry Avenue North, Seattle, WA 98109-5210 U.S.A.

[1] Excludes professional services, for which the applicable AWS Contracting Party is Amazon Web Services, Inc. Additionally, this applies only if your purchase on AWS Marketplace is from a third party that has been onboarded to Amazon Web Services EMEA SARL. Otherwise, Amazon Web Services, Inc. is the applicable AWS Contracting Party.

20.1.7. If you are an AWS customer located in India, parties agree that this Section 20.1.7 will be applicable:

20.1.7.1. If you have provided your Goods and Services Tax (GST) registration number to us so that it can be applied to your purchases, then the information you provide with your registration (including your GST registration number and the name and address associated with your GST registration) will be shared with third parties from whom you have purchased software on the AWS Marketplace to the extent necessary for those third parties to comply with GST invoicing regulations and requirements.

20.1.7.2. The purchase fees and charges payable by you will be exclusive of all applicable Taxes, and will be made free and clear of any deduction or withholding, as may be required by law. For clarity, if any such deduction or withholding (including but not limited to cross-border withholding taxes) is required on any payment, you will pay such additional amount, as necessary, to ensure that the net amount received by AWS or its affiliates is equal to the amount then due and payable by you for your purchases on the AWS Marketplace. AWS or its affiliates will provide you with such tax forms, as are reasonably requested, in order to reduce or eliminate the amount of any withholding or deduction for taxes, in respect of the payments made by you for purchases on the AWS Marketplace. AWS or its affiliates may charge, and you will pay, all applicable Taxes that it or we are legally obligated or authorized to collect from you. AWS or its affiliates will not collect, and you will not pay, any Taxes for which you furnish us a properly completed exemption certificate, or a direct payment permit certificate, for which AWS or its affiliates may claim an available exemption from such Taxes.

20.2. Seller Terms. If you promote, license, sell, provide or provide access to any Content or services through AWS Marketplace, the Service Terms for AWS Marketplace Sellers apply to you.

21. AWS Ground Station

21.1. Any guidance provided through Licensing Accelerator or by AWS Ground Station is provided for your convenience, does not constitute legal or compliance advice, and is not subject to any legal professional privilege. You are responsible for making your own assessment of whether your use of AWS Ground Station meets applicable legal and regulatory requirements, including by engaging with a legal professional if necessary.

21.2. You will not, and will not allow any third-party to, use Licensing Accelerator or AWS Ground Station to, directly or indirectly, develop or improve a similar or competing product or service.

21.3. You are solely responsible for applying appropriate security measures to your space assets and the data transmitted to and from your space assets, including using encryption, firewalls, and other network security tools as appropriate, and not allowing unauthorized access to your data.

21.4. You represent and warrant that you own all right, title, and interest in, or have all necessary authority to permit use of, any space assets associated with your AWS account, and you agree to provide to AWS, upon request, documentation demonstrating such ownership or authority. AWS is not a party to any agreement you have or may enter into with any other individual or entity accessing or using the Services, any of Your Content, or any space assets associated with your account. You are solely responsible for your separate relationship with any such individual or entity.

21.5. If your AWS Contracting Party is AWS Serviços Brasil Ltda., AWS Ground Station continues to be sold and provided to you by Amazon Web Services, Inc. (or other entity identified as applicable); but AWS Serviços Brasil Ltda. remains your AWS Contracting Party under the Agreement.

22. Amazon Elastic Transcoder

The distribution of files created by Amazon Elastic Transcoder may require that you obtain license rights from third parties, including owners or licensors of certain third party audio and video formats. You are solely responsible for obtaining these licenses and paying any necessary royalties or fees.

23. AWS OpsWorks

23.1. Your use of the AWS OpsWorks agent is governed by the AWS OpsWorks Client License Agreement. Your use of AWS OpsWorks for Chef Automate is subject to Chef Software Inc.'s end user license agreement. Your use of AWS OpsWorks for Puppet Enterprise is subject to Puppet, Inc.'s Puppet Enterprise License Agreement.

23.2. Your use of AWS OpsWorks for Chef Automate and AWS-ApplyChefRecipes, which leverage the Chef Infra Client software, are subject to Progress Software Corporation's Online Master License and Services Agreement for Chef (the "Progress EULA") except that sections 1.9.2. (Product Compliance with Documentation) and 1.10.1. (Our Indemnification Obligation) of the Progress EULA do not apply and the Product, Documentation, and Technology (all as defined in the Progress EULA) are provided "as is," with all faults, and Progress Software Corporation disclaims all warranties, express or implied, including, but not limited to, warranties of merchantability, fitness for a particular purpose, title, noninfringement, availability, error-free or uninterrupted operation, and any warranties arising from course of dealing, course of performance, or usage of trade. To the extent that Progress Software Corporation may not as a matter of applicable law disclaim any implied warranty, the scope and duration of such warranty will be the minimum permitted under applicable law.

24. AWS Supply Chain

24.1. You agree and instruct that we may use Your Content that is processed by AWS Supply Chain to generate forecasts, insights, or recommendations to you.

24.2. You and your End Users are responsible for all decisions made, advice given, actions taken, and failures to take action based on your use of AWS Supply Chain. AWS Supply Chain uses machine learning models that generate predictions based on patterns in data. Output generated by a machine learning model is probabilistic and should be evaluated for accuracy as appropriate for your use case, including by employing human review of such output.

24.3. You agree and instruct that for AWS Supply Chain: (a) we may use and store Your Content that is processed by the AWS Supply Chain service to develop and improve the service and its underlying technologies; (b) we may use and store Your Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial-intelligence technologies; and (c) solely in connection with the development and improvement described in clauses (a) and (b), we may store Your Content in an AWS region outside of the AWS region where you are using AWS Supply Chain. You may instruct AWS not to use and

store Your Content processed by AWS Supply Chain to develop and improve the AWS Supply Chain service or technologies of AWS or its affiliates by following the instructions set forth in the "Opt-out policy" section of AWS Supply Chain administrative guide.

24.4. You are responsible for providing legally adequate privacy notices to End Users of AWS Supply Chain and obtaining any necessary consent from such End Users for the processing of Content and the storage, use, and transfer of Content as described under this Section 24.

24.5. If you have been onboarded to the AWS Supply Chain N-Tier Visibility Service by your customer (Your Customer), the following applies to Your Content that is within the N-Tier Visibility Service:

24.5.1. Your Content will be stored in the same AWS region where Your Customer's Content is stored.

24.5.2. If Your Customer terminates its use of the AWS Supply Chain N-Tier Visibility Service, you will be notified of that termination and you will have 30 days following that termination to retrieve Your Content from the Service if you choose to do so, after which time Your Content will be removed.

24.6. Amazon Q in AWS Supply Chain. Section 50 below applies to Amazon Q in AWS Supply Chain.

25. Amazon AppStream 2.0

25.1. NVIDIA Software. If your application uses the NVIDIA graphics processing unit (GPU) on an Amazon AppStream 2.0 instance, your use is subject to the terms and conditions of the NVIDIA Cloud End User License Agreement.

25.2. If you use the Amazon AppStream 2.0 User Pool feature to enable End Users to access applications, you agree that we may store and process these End Users' email addresses in AWS Regions outside the AWS Regions where you are using Amazon AppStream 2.0. We will only use these email addresses to send the End Users email notifications to enable them to access Amazon AppStream 2.0.

26. Amazon WorkSpaces

26.1. Any Content that you or any End User run on, cause to interface with, or upload to your WorkSpaces is Your Content. You are responsible for maintaining licenses and adhering to the license terms of any of Your Content on your WorkSpaces.

26.2. Use of Microsoft Software on Amazon WorkSpaces is subject to Section 5.1 above. Microsoft is an intended third-party beneficiary of this Section 26.2, with the right to enforce its provisions.

26.3. Amazon WorkSpaces is designed to serve as a cloud desktop service. WorkSpaces may not be used to accept inbound network connections, as server instances, or to serve web traffic or your network traffic, and you may not reconfigure the inbound network connections of your WorkSpaces.

26.4. You and End Users may only use the WorkSpaces client software on computer equipment owned or controlled by you or your End Users. Your use of the WorkSpaces client software is governed by the Amazon WorkSpaces Application License Agreement.

26.5. To perform configurations, health checks, and diagnostics on Amazon WorkSpaces, we may collect and use performance and log information tied to the operation and management of the Service.

26.6. Software installed by us on your WorkSpaces may connect to a license activation server hosted by AWS. You may not attempt to prevent any license activation function.

26.7. As part of regular operation of Amazon WorkSpaces, WorkSpaces may be updated with operating system and software upgrades, patches, and bug fixes. During these updates, only software, documents, and settings that are part of the operating system image used for the WorkSpace or part of a user's profile (D: drive in the WorkSpace) will persist.

26.8. Microsoft BYOL Licensing. Under this option, Amazon WorkSpaces enables you to provision WorkSpaces using your Microsoft Software and Microsoft Licenses (the "WorkSpaces BYOL Program"). You must be eligible to use the WorkSpaces BYOL Program for the applicable Microsoft software under your agreement(s) with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. Further, your use of Microsoft Software under the WorkSpaces BYOL Program is subject to the applicable Microsoft licensing requirements, including Microsoft's End User License Agreement (Microsoft EULA). You agree that you have determined that your use of the WorkSpaces BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted.

27. Amazon Cognito

27.1. We may change, discontinue, or deprecate support for any third-party identity provider at any time without prior notice.

27.2. In the event a particular Cognito User Pool has no active users within a 12 month period, we may delete the Cognito User Pool upon 30 days' prior notice to you.

28. Amazon WorkDocs

28.1. Portions of Amazon WorkDocs in Japan are sold and provided by AMCS LLC, an affiliate of AWS, and not AWS, but is otherwise subject to the terms of the Agreement.

28.2. We may delete any of your End Users' Content uploaded to Amazon WorkDocs if the End User is marked "Inactive" in the Amazon WorkDocs' Administrator Dashboard and you have not been billed for more than 30 days for this End User's usage. We may also delete your Amazon WorkDocs site and Your Content when you have no End Users marked "Active" within the Amazon WorkDocs Administrator Dashboard for more than 30 days.

28.3. If no End User accounts associated with your AWS account have registered any usage of the Services for several months, then we may delete the inactive End Users' accounts after providing 30 days' notice.

28.4. Your use of the Amazon WorkDocs Sync Software is governed by the Amazon WorkDocs Sync License Agreement.

28.5. Your use of the Amazon WorkDocs Application is governed by the Amazon WorkDocs Application License Agreement.

28.6. Open with Office 365 is Third-Party Content provided by Microsoft. By using Open with Office 365, you are subject to Microsoft's terms of use and privacy policy. You are solely responsible for obtaining all required licenses from Microsoft to use Open with Office 365 and for complying with all applicable Microsoft licensing requirements.

28.7. The Hancom document editing service is Third-Party Content. Your use of the Hancom document editing service through Amazon WorkDocs is subject to the Hancom Terms of Service. If you do not accept the Hancom Terms of Service applicable to the Hancom document editing service, then do not enable and use the Hancom document editing service. If you enable and use the Hancom document editing service, Hancom will have access to the contents of the document being edited and the End User's user name and profile picture. Hancom is only authorized by AWS to access the above information for the purpose of providing the Hancom document editing service and only for the duration of the editing session.

28.8. AWS is the registrant of, and controls the DNS records for, all [name].workdocs.aws domain names ("Domain Names"). Customer does not acquire any rights in any such domain. Termination or suspension of Customer's AWS account may result in the termination or suspension of Customer's ability to use its previously assigned Domain Names. In order to use a Domain Name, Customer must comply with all guidelines included in the Amazon WorkDocs Site Naming Policy.

29. Amazon Pinpoint and AWS End User Messaging (formerly, the SMS, MMS, voice message, and push notification features of Amazon Pinpoint)

29.1. Portions of Amazon Pinpoint and AWS End User Messaging in Japan are sold and provided by AMCS LLC ("AMCS"), an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

29.2. Portions of Amazon Pinpoint and AWS End User Messaging in Singapore are sold and provided by AMCS SG PRIVATE LIMITED ("AMCS SG"), an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

29.3. Amazon Pinpoint and AWS End User Messaging utilize underlying functionality from Amazon Simple Email Service (SES), and your use of Amazon Pinpoint and AWS End User Messaging is subject to the terms that govern Amazon Simple Email Service (SES).

29.4. You acknowledge that Amazon Pinpoint and AWS End User Messaging:

a. Are not Integrated Public Alert and Warning System (IPAWS) eligible systems.

b. Are not intended for use in, or in association with, the operation of any hazardous environments or critical systems. You are solely responsible for liability that may arise in association with such use.

c. Do not support or carry emergency calling or messaging to any emergency services personnel or public safety answering points ("Emergency Services"), such as calls or texts to 911, and may not determine the physical location of your devices or your End Users, which may be required when contacting Emergency Services. You understand and agree that it is your responsibility to: (i) contact and access Emergency Services independently of Amazon Pinpoint and/or AWS End User Messaging; and (ii) inform all End Users of these limitations.

d. Are not replacements for traditional telephone or mobile phone services, including but not limited to calling, texting, or contacting Emergency Services, and do not function as such.

29.5. Through your use of AWS End User Messaging you will not:

- Offer or purport to offer any Emergency Services. "Emergency Services" means services that allow a user to connect with emergency services personnel or public safety answering points, such as 911 or E911 services.
- If the applicable AWS Contracting Party is AWS India, "Emergency Services" shall mean services that allow a user to connect with emergency services personnel or public safety answering points, such as 100, 112 services.
- Transmit material that is sexually explicit, relates to "adult services", or contains sensitive financial or identifying information (such as social security numbers).

- Resell, sublicense, or timeshare the Services, or use them on behalf of anonymous or other third parties

29.6. From time to time, telecommunication providers may change or modify their rules, requirements, and policies (collectively "Carrier Policies"). We will make reasonable efforts to notify you of changes to Carrier Policies through, for example, email, Personal Health Dashboard notifications, or technical documentation. You are responsible for complying with all Carrier Policies that apply to your use of the Service.

29.7. Fees for Amazon Pinpoint and AWS End User Messaging will apply regardless of whether delivery of your messages is prevented, delayed, or blocked due to reasons outside of our control.

29.8. You are responsible for complying with legal requirements related to unsolicited or unwanted communications, including without limitation, the Telephone Consumer Protection Act (TCPA), the FTC's Telemarketing Sales Rule, and the EU e-Privacy Directive, or any other similar telemarketing law.

29.9. We may change, discontinue, or deprecate support for a third party push notification platform at any time. We will provide you with prior notice of any deprecation or discontinuation of support for a third party push notification platform where practicable under the circumstances.

29.10. If the applicable AWS Contracting Party is AWS India, you must obtain our prior written consent before using AWS End User Messaging to send SMS messages for:

- financial transactions or payment services (e.g., mobile banking, bill presentment, bill payment, money transfer, peer-to-peer payment or lending credit, debit or stored value payment services);
- sweepstakes or contests; or
- advertisements or promotions for commercial products, goods, or services.

29.11. To enable WhatsApp messaging integration with AWS End User Messaging, you must create a WhatsApp Business Account ("WABA") and are responsible for reviewing and accepting any applicable Meta and WhatsApp terms related to the WhatsApp Business Solution. You understand that any content, information, and data you upload to, and any messages you send or receive using, the WhatsApp Business Solution are processed by Meta in order to provide the Service. You agree that you are solely responsible for your or your End User's use of the WhatsApp Business Solution, the content you or your End Users send through the WhatsApp Business Solution, and compliance with applicable Meta or WhatsApp terms.

29.12. Your use of the AWS End User Messaging Service in certain countries is subject to additional Country Specific Communications Service Terms.

30. AWS Lambda

We may delete, upon 30 days' notice to you, any of Your Content uploaded to AWS Lambda if it has not been run for more than 3 months. You may only use Lambda's storage resources to store function code (compiled or uncompiled), dependencies (e.g. layers), and related configuration and meta-data, as necessary to execute your code on Lambda (per the technical documentation). Any other use, including but not limited to, using Lambda's storage for the purpose of hosting generally accessible content for download or storage, is not permitted and may result in us deleting Your Content.

31. Amazon WorkMail

31.1. When you use Amazon WorkMail, you also use AWS Key Management Service, AWS IAM, and Amazon SES, and your use of Amazon WorkMail is subject to the terms that govern those Services.

31.2. Amazon WorkMail provides a filtering service designed to filter unwanted emails, such as spam, phishing emails, and email infected with viruses. You acknowledge that the technological limitations of the filtering service will likely result in the capture of some legitimate email and the failure to capture some unwanted email, including email infected with viruses.

31.3. Your mail domain and End Users' accounts may be blocked, delayed, or prevented from being delivered by destination email servers and other reasons outside of our control. Your payment obligations continue regardless of whether delivery of your emails is prevented, delayed, or blocked.

31.4. You agree not to use Amazon WorkMail for sending:

- Bulk emails, such as mass marketing emails
- Unsolicited and unwanted emails
- Phishing emails

31.5. You are solely responsible for ensuring any emails you or your End Users send using Amazon WorkMail comply with the CAN-SPAM Act and all other applicable law. You agree that AWS is not the "sender" of any emails you or your End Users send using Amazon WorkMail as defined in the CAN-SPAM Act and all other applicable laws.

31.6. Amazon WorkMail may log and use information such as server hostnames, IP addresses, timestamps, mail queue file identifiers, and spam filtering information for the purpose of troubleshooting or improving Amazon WorkMail.

31.7. If your use of Amazon WorkMail is terminated, we may delete your data and your End Users' mailboxes.

31.8. Portions of Amazon WorkMail in Japan are sold and provided by AMCS LLC, an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

32. Amazon WorkSpaces Application Manager (Amazon WAM)

32.1. When you use Amazon WAM, you also use Amazon WorkSpaces, and your use is subject to the terms that govern Amazon WorkSpaces.

32.2. You may use the Amazon WAM Admin Studio only to package applications, and the Amazon WAM Admin Player only to validate applications, that will be delivered via Amazon WAM to your WorkSpaces.

32.3. As part of regular operation of Amazon WAM, we may update your Amazon WAM desktop applications with software upgrades, patches, and bug fixes.

33. AWS B2B Data Interchange

33.1. When you register as a trading partner to access an AWS B2B Data Interchange Portal established under another AWS account ("B2B Data Interchange Portal"), you are an End User of that AWS account. Content you contribute to a B2B Data Interchange Portal ("Trading Partner Contributed Content") as an End User is not considered Your Content for the purposes of rights and obligations under the terms of this Agreement. Subject to the non-exclusive license granted by Section 33.2, this does not modify any rights you may hold in your Trading Partner Contributed Content.

33.2. Trading Partner Contributed Content may be viewed by others who have access to the B2B Data Interchange Portal. Unless you enter into a license with other parties who have access to the B2B Data Interchange Portal specifying different terms, you grant each party who has access a nonexclusive, worldwide, irrevocable license, without restriction, to use the Trading Partner Contributed Content. You represent and warrant that you have all rights necessary to grant this license.

33.3. When you invite another party to register as a trading partner to access your B2B Data Interchange Portal, they become an End User of your AWS account and their Trading Partner Contributed Content is considered Your Content under the terms of the Agreement. You are responsible for the conduct of End Users that you invite, including their Trading Partner Contributed Content.

34. AWS Directory Service

Use of Microsoft Software on AWS Directory Service is subject to Section 5.1 above. Microsoft is an intended third-party beneficiary of this Section 34, with the right to enforce its provisions.

35. AWS Device Farm

35.1. For any test run on an Apple device (each, an "Apple Test"), you represent and warrant that you have an active and valid registered Apple Developer Account under your iOS Developer Program License Agreement with Apple at the time any such Apple Test is run. You appoint us as your Authorized Developer (as defined in the Apple Developer Program License Agreement) for the duration of all Apple Tests and understand that you are responsible to Apple for all actions we undertake in connection with each Apple Test.

35.2. You agree not to and not to attempt to:

(i) perform any network discovery inside the AWS Device Farm or otherwise in connection with the test;

(ii) generate any internet traffic from within the EC2 instances of AWS Device Farm, unless approved by us; internet traffic should be limited to devices only;

(iii) root, unlock, or jailbreak any Device Farm device;

(iv) install persistent software on devices or EC2 instances; or

(v) factory reset or change settings on devices, or call or access third-party servers in a manner that would interfere with any Services.

35.3. You acknowledge and agree that we may disclose application packages, test packages (pre- compiled), test script source code, application extension files, or auxiliary data files to third parties solely for purposes of conducting automated security verification.

36. Amazon OpenSearch Service

Amazon OpenSearch Service creates daily automated snapshots of your Amazon OpenSearch Service domains. We will maintain these automated snapshots for a period of at least 14 days after they are created. We may delete automated snapshots at any time after 14 days.

37. AWS Database Migration Service

37.1. The AWS Database Migration Service (DMS), including DMS Fleet Advisor and the AWS Schema Conversion Tool, is AWS Content under the Intellectual Property License, and you and all End Users may install and/or use it solely for the purpose of migrating or moving data, provided that: (i) at least one of the

source data store and target data store resides in AWS; and (ii) the source and target data stores are both listed in the DMS documentation of supported sources and targets.

37.2. The AWS Database Migration Service (DMS), including DMS Fleet Advisor and the AWS Schema Conversion Tool, collects performance metrics and usage patterns, including: the types of database engines and related configurations used; number of rows processed; and information related to schema, queries, compatibility, performance, and task duration and status; which when combined with database license and feature information are used to provide, maintain, and improve the quality of the Services and recommendations on potential database engine and instance migrations. DMS Fleet Advisor collects information about resources on your network that you designate for discovery.

38. AWS Amplify

You must have all necessary rights to use any domain name that you use in conjunction with AWS Amplify.

39. AWS IoT Services

39.1. "AWS IoT Services" means AWS IoT Core, AWS IoT Device Management, AWS IoT Device Defender, AWS IoT 1-Click, AWS IoT Events, AWS IoT Analytics, AWS IoT SiteWise, AWS IoT FleetWise , AWS IoT TwinMaker, FreeRTOS, AWS IoT ExpressLink, Amazon Kinesis Video Streams, and AWS IoT Greengrass.

39.2. AWS IoT Services are not designed or intended for, and may not be used for, any use case where any error, defect, unavailability, or other deficiency or failure of any AWS IoT Service could lead to bodily injury or death or cause environmental or property damage. You are solely responsible for: (a) using AWS IoT Services in a manner that is safe and compliant with applicable laws and industry-specific requirements and standards; (b) testing your use of AWS IoT Services (such as any delivery of remote commands) prior to deployment in your products and services, and ongoing monitoring of your use of AWS IoT Services thereafter; (c) any recalls and corrective action for your or your End Users' products and services that use AWS IoT Services; and (d) any other liability arising from your use of AWS IoT Services in violation of this paragraph.

39.3. You may not rely on data collected through your use of AWS IoT Services as a substitute for any human monitoring of physical systems necessary to assess whether such systems are operating properly or safely.

39.4. AWS IoT Core Device Shadow data for an individual device may be deleted if you do not update the Device Shadow data for an individual device within any given 12-month period. AWS IoT Core Device Registry data for an individual device may be deleted if you do not update the Registry data for an individual device within any given 7-year period. Once Device Shadow or Registry data has been updated for an individual device the data restriction time frame for that individual device resets, and the Device Shadow and Registry data storage time frame for an individual device starts over.

39.5. You are responsible for the creation, distribution, and security (including enabling of access) of any IoT devices connected to or enabled by your AWS account.

39.6. The AWS IoT FleetWise Edge Agent Reference Implementation is intended to help you develop your Edge Agent for AWS IoT FleetWise and includes sample code that you may reference or modify so your Edge Agent meets your requirements. You are solely responsible for your Edge Agent, including ensuring that your Edge Agent and any updates and modifications thereto are deployed and maintained safely and securely in any vehicles.

39.7. AWS IoT ExpressLink is AWS cloud connectivity software and specifications that select AWS Partner Network (APN) Partners may incorporate into hardware modules they develop, manufacture, and offer to AWS customers. If you purchase a hardware module (including any evaluation kit) from an APN Partner that includes AWS IoT ExpressLink, you agree that AWS is not a party to any agreement between you and the APN Partner governing your purchase and use of the module, AWS is not responsible or liable to you for the module, and AWS does not make any representations or warranties with respect to the module.

39.8. The FreeRTOS Extended Maintenance Plan ("FreeRTOS EMP") provides subscribing customers with security patches and critical bug fixes on a chosen FreeRTOS Long Term Support (LTS) version beyond the expiry of that version's initial LTS period. FreeRTOS EMP is a "Service" for purposes of the Agreement. Any code, fixes or patches (collectively, "EMP Patches") that you receive, obtain or access in connection with FreeRTOS EMP that have not been incorporated into the publicly available FreeRTOS libraries are AWS Content provided to you under the Intellectual Property License, except that AWS also grants you a limited, non-exclusive, non-sublicensable, non-transferrable, perpetual license to (a) modify and create derivative works of the EMP Patches and (b) to distribute the EMP Patches in object code form only.

39.9. If you use Semtech as your geolocation provider in the AWS IoT Core Device Location feature, you authorize AWS to transmit your geolocation request parameters (e.g., location data used to run the location solvers) and/or resulting output data generated by the feature (e.g., geographic coordinates) to Semtech for troubleshooting and diagnostic purposes, and other technical support. Semtech may be outside of the AWS region in which you were using the feature. If you use HERE as your geolocation provider in the AWS IoT Device Core Location feature, the terms in Sections 82.1-82.5, 82.7-82.8, and 82.10 apply. AWS may deprecate or discontinue any geolocation provider within the feature at any time upon notice to you.

39.10. "AWS IoT Core for LoRaWAN Public Network Support" is a feature of AWS IoT Core that helps customers connect their LoRaWAN devices to AWS using a publicly available LoRaWAN network ("Public LoRaWAN Network"), which is provided as a service by a third-party network provider ("LoRaWAN Network Provider"). The LoRaWAN Network Provider is solely responsible for the operation and security of its Public LoRaWAN Network (including its gateways and any other equipment), which is separate from and located outside of AWS data center facilities, servers, networking equipment, storage media, and host software systems. Your use of Everynet BV's Public LoRaWAN Network is subject to their terms and conditions. AWS has no control over, and makes no guarantees about, any Public LoRaWAN Network.

If you use this feature, you authorize AWS to transmit to the LoRaWAN Network Provider device identification codes and related device information so the LoRaWAN Network Provider can receive and transmit device messages, and provide support. AWS may change, deprecate, or discontinue the availability of the LoRaWAN Network Provider through AWS IoT Core at any time upon notice to you.

39.11. AWS IoT Core for Amazon Sidewalk

39.11.1. "AWS IoT Core for Amazon Sidewalk" is a feature of AWS IoT Core that enables customers to build applications and devices that connect to a shared network of bridge devices ("Gateways") that contribute low-bandwidth connection to Amazon Sidewalk-enabled devices to help extend their working ranges and stay connected to the internet ("Amazon Sidewalk"). Amazon Sidewalk is provided by Ring LLC, however usage of and connectivity to Amazon Sidewalk from AWS is included as a part of AWS IoT Core for Amazon Sidewalk. You agree to, and must comply with, the following (which can be found in the Amazon Sidewalk User Guide): (i) the Amazon Sidewalk Program Requirements; (ii) the Works with Amazon Sidewalk Qualification Guidelines; and (iii) the Amazon Sidewalk Program Security Requirements. We may suspend or terminate Amazon Sidewalk and/or your access to it at any time without prior notice.

39.11.2. You may not sell, distribute, or otherwise make available any device, component, or other product that connects to, enables connectivity to, or interacts with Amazon Sidewalk (an "AS Device") unless that AS Device has been and remains qualified at all times through the Works with Amazon Sidewalk ("WWAS") qualification program.

39.11.3. We may collect and use certain information related to your AS Devices, including transmission and authentication identifiers. We use this data for purposes of maintaining and providing AWS IoT Core for Amazon Sidewalk. You provide specific authorization for AWS to use Ring LLC as a sub-processor in accordance with the DPA to process Customer Data in the US in order to make Amazon Sidewalk available for this feature.

39.11.4. Gateways are owned by customers who are contributing bandwidth from their Gateway's existing internet service to Amazon Sidewalk, and are separate from and located outside of AWS data center facilities, servers, networking equipment, storage media, and host software systems. Consequently, (i) you are responsible for ensuring the security of your products and services in connection with their usage of or connectivity to Amazon Sidewalk, (ii) any commitments made in the Agreement related to security do not apply to Amazon Sidewalk, and (iii) Amazon Sidewalk coverage, density, bandwidth, up-time, and availability is not guaranteed and may change without notice.

39.11.5. Subject to your compliance at all times with the Agreement and the Works with Amazon Sidewalk Badge Guidelines, we hereby grant you a non-exclusive, royalty-free, and revocable license to use AWS Marks provided to you in connection with the WWAS qualification program (collectively, the "WWAS Marks"), to identify your WWAS-qualified AS Devices as using or being compatible with Amazon Sidewalk. Your use of WWAS Marks is also subject to Sections 4-7, 9, 11, and 14-18, of the AWS Trademark Guidelines. You must include the following statement in any materials that display the WWAS Marks: "Amazon,

Amazon Sidewalk, and all related marks are trademarks of Amazon.com, Inc. or its affiliates." We may include information about you and your AS Devices in our marketing materials to identify you as a participant in the WWAS program, including your name, logo, images, and videos of your AS Devices.

40. Amazon QuickSight

40.1. You may enable End Users to use Amazon QuickSight under your account. If you choose to enable End Users under your account, it is your responsibility to inform each End User that our termination of your use of Amazon QuickSight will also terminate their use of Amazon QuickSight. It is also your responsibility to inform them that you are acting as an "Amazon QuickSight Administrator" and can perform the following actions: (a) activate and deactivate End Users' Amazon QuickSight accounts; (b) control End User access to data sets and certain functionality of Amazon QuickSight; and (c) access information about End Users' use of Amazon QuickSight.

40.2. Amazon QuickSight may use Your Content that you select as a data source for Amazon QuickSight to make personalized recommendations to you, such as suggested visualizations based on your query history and suggested insights.

40.3. Amazon QuickSight Machine Learning Services. Section 50 below applies to Amazon Q in QuickSight (formerly known as Amazon QuickSight Q).

40.4. QuickSight Readers. Readers (as defined in the QuickSight documentation) that are used for automatically or programmatically refreshing dashboards for near real-time use cases must choose capacity pricing. For readers under user pricing, each reader is limited to manual use by one individual only.

41. AWS Certificate Manager

41.1. By using AWS Certificate Manager ("ACM") you authorize us, Amazon Trust Services, LLC ("ATS"), or our affiliates (collectively, "Amazon CA") to apply for and obtain publicly trusted SSL/TLS certificates (each, a "Certificate") from certification authorities located in the United States, some of whom may be third parties, for the domain name you provide to us. By submitting a request for a Certificate, you certify that (1) you are the Domain Name Registrant (as defined in the then current CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (the "CA/B Forum Requirements" located here); (2) you have control over the Fully-Qualified Domain Name (as defined in the CA/B Forum Requirements); or (3) you have been granted authority by the Domain Name Registrant to authorize Amazon CA to apply for and obtain each Certificate. You acknowledge that, solely for purposes of obtaining the Certificate and for no other purposes, you are giving Amazon CA control over the Fully-Qualified Domain Name, and you approve of Amazon CA requesting the Certificate for the domain name. We may decline to provide you with a Certificate for any reason.

41.2. You agree that:

(i) All information you provide in connection with your use of Certificates is and will be accurate and complete information at all times (and you will promptly notify us if your information changes);

(ii) You will review and verify the Certificate for accuracy;

(iii) You may use a Certificate we provide to you solely on servers that are accessible at the subjectAltName(s) listed in the Certificate and will use the Certificate solely in compliance with all applicable laws;

(iv) You will promptly cease using a Certificate, and promptly notify us, in the event that any information in the Certificate is incorrect or inaccurate;

(v) You will promptly cease using a Certificate, and promptly notify us, if the private key associated with the Certificate is subject to a Key Compromise (as defined in the CA/B Forum Requirements) or the Certificate is otherwise subject to misuse;

(vi) You will promptly respond to Amazon CA's instructions concerning Key Compromise or Certificate misuse;

(vii) You will not modify, sublicense, or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or Private Key;

(viii) You will not, in connection with use of the Certificate, upload or distribute any files or software that may damage the operation of another's computer;

(ix) You will not make representations about or use a Certificate except as may be allowed in ATS's CPS;

(x) You will not, in connection with use of the Certificate, impersonate or misrepresent your affiliation with any entity;

(xi) You will not permit an entity other than Amazon CA to control the Private Key matching the Public Key in the Certificate (where "Private Key" and "Public Key" are defined by the CA/B Forum Requirements);

(xii) You will not use a Certificate to breach the confidence of a third party or to send or receive unsolicited bulk correspondence; and

(xiii) You acknowledge that Amazon CA (or our applicable third-party contractor) may revoke a Certificate at any time, and you agree that you will cease using the Certificate immediately upon our notice of such revocation.

42. AWS Verified Access

42.1. We may change, discontinue, or deprecate support for any third-party trust provider at any time without prior notice.

43. Amazon GameLift

43.1. You may only access or use Amazon GameLift for video game server hosting; provided however, that this restriction does not apply to your use of the FlexMatch feature independent of other Amazon GameLift features.

43.2. We or our affiliates may delete, upon 30 days' notice to you, any of Your Content uploaded to Amazon GameLift if it has not been run in more than 3 months.

43.3. Your use of Amazon GameLift Local is governed by the Amazon GameLift Local License Agreement.

43.4. The Amazon GameLift Spot Instance program allows you request that certain Amazon GameLift instances run pursuant to the Amazon GameLift Spot instance pricing and payment terms set forth on the Amazon GameLift product detail page on the Site (each requested instance, a "GL Spot Instance"). We may terminate the Amazon GameLift Spot Instance program at any time. We may terminate, stop, or hibernate GL Spot Instances at any time and without any notice to you for AWS capacity requirements. You should configure your game to ensure it is fault tolerant and will correctly handle interruptions. GL Spot Instances may not be used with certain Services, features and third-party software we specify, including those listed in Section 5.3, above.

44. AWS Application Discovery Service

When you use AWS Application Discovery Service, data that is scanned by AWS Application Discovery Service in your on-premises computing resources will be deemed Your Content.

45. AWS Professional Services

45.1. "AWS Professional Services" are advisory and consulting services that AWS provides under a statement of work ("SOW") to help you use the other Services. AWS Professional Services are "Services" for purposes of the Agreement.

45.2. AWS or any of its affiliates may enter into a SOW or an addendum to the Agreement with you to provide AWS Professional Services. For the purposes of each SOW or addendum, the term "AWS" in the SOW, the addendum and the Agreement refers to the AWS entity that executes the SOW or addendum, and no

other AWS entity has any obligations under that SOW or addendum. Each SOW or addendum (together with the Agreement) is intended by the parties as the final, complete, and exclusive terms of their agreement and supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to the subject matter of that SOW or addendum.

45.3. AWS will invoice you monthly for the AWS Professional Services. Payments for AWS Professional Services are not refundable.

45.4. AWS does not provide legal or compliance advice. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

45.5. Other than Third Party Content, Content that AWS provides as part of the AWS Professional Services is AWS Content. You are solely responsible for testing, deploying, maintaining and supporting Content provided or recommended by AWS.

45.6. AWS may develop Content consisting of either (a) documents and diagrams ("Documents") or (b) software (in source or object code form), sample code, or scripts ("Software") for you as part of the AWS Professional Services (such Documents and Software, "Developed Content"). Subject to any non- Disclosure agreement in effect between you and AWS, AWS is not precluded from developing, using, or selling products or services that are similar to or related to the Developed Content. Any Developed Content provided to you by AWS as part of the AWS Professional Services under a SOW is licensed under the following terms:

- AWS licenses any Documents to you under the Creative Commons Attribution 4.0 International License (CC-BY 4.0); and
- AWS licenses any Software to you under the Apache License, Version 2.0.

45.7. Some Developed Content may include AWS Content or Third Party Content provided under a separate license. In the event of a conflict between Section 45.6 above and any separate license, the separate license will control with respect to such AWS Content or Third Party Content.

45.8. Any materials or information that you own or license from a third party and provide to AWS for the purposes of the AWS Professional Services are Your Content. If you choose to provide access to Your Content to AWS, then you will ensure that you have adequate rights and permissions to do so.

45.9. If there is a conflict between this Section 45 and any AWS Implementation Services Addendum between you and AWS, the terms of the AWS Implementation Services Addendum will control, and references to "Implementation Services" in that addendum include AWS Professional Services.

45.10. AWS and its affiliates will handle any personal data relating to your personnel ("Personnel") that is provided to AWS or its affiliates in connection with a SOW in accordance with the handling practices described in the AWS Privacy Notice (available at https://aws.amazon.com/privacy/). You will make the AWS Privacy Notice available to any Personnel whose personal data you provide to AWS or its affiliates.

46. Amazon Redshift

The Reserved Node program allows you to designate Amazon Redshift nodes as subject to the reserved pricing and payment terms set forth on the Amazon Redshift pricing page on the AWS Site (each designated node, a "Reserved Node"). We may terminate the Reserved Node program at any time. We may change pricing for the Reserved Node Program at any time, but price changes will not apply to previously designated Reserved Nodes. Reserved Nodes are noncancellable, and you will owe the amount charged for the Reserved Node for the duration of the term you selected, even if the Agreement is terminated. Reserved Nodes are nontransferable, and all amounts paid in connection with Reserved Nodes are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved Node type, or terminate the Reserved Node program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved Node. Upon expiration or termination of the term of a Reserved Node, the Reserved Node pricing will expire and standard on-demand usage prices will apply to the Amazon Redshift node.

47. AWS Server Migration Service

47.1. When you use AWS Server Migration Service, data that is scanned by AWS Server Migration Service in your on-premises computing resources will be deemed Your Content.

47.2. We may terminate the migration of any image that remains in a migration queue for 90 days or more.

48. AWS Organizations

48.1. AWS Organizations enables you to create an "Organization" by joining a single AWS account (the "Management Account," previously called the "Master Account") with one or more AWS accounts (each, a "Member Account"). Except as authorized by AWS, only AWS accounts used by you, your affiliates, your employees, or your subcontractors currently doing work on your behalf may be joined in an Organization. By joining an Organization as a Member Account, you agree: (a) to disclose billing, account activity, and account information of the Member Account to the Management Account; and (b) that the Management Account may purchase EC2 Reserved Instances on a Member Account's behalf.

48.2. If you enable consolidated billing, the Management Account and Member Account will be jointly and severally liable for all charges accrued by the Member Accounts while joined in an Organization, but the Management Account will be billed for all such charges in accordance with the Management Account's Agreement. If a Management Account is suspended for non-payment, then all Member Accounts in the Organization will be suspended.

48.3. We may enable, with at least 14 days' prior notice to you, all features in your Organization if requested by the Organization's Management Account. If your Organization has all features enabled: (i) the consolidated billing terms as described in Section 48.2 will apply to your Organization; (ii) the Management

Account will have full access to and control over its Member Accounts; and (iii) the Management Account is jointly and severally liable for any actions taken by its Member Accounts.

48.4. When a Management Account uses AWS Organizations or the CreateLinkedAccount API to create an account ("Created Account"): (i) the Created Account will be a Member Account of the Management Account's Organization with the AWS Organizations features that the Management Account enables from time to time; (ii) the Created Account is governed by the terms of the Management Account's Agreement; (iii) the Management Account is jointly and severally liable for any actions taken by the Created Account; and (iv) an IAM role is created in the Created Account that grants the Management Account full administrative access to the Created Account.

49. Amazon Athena

Notwithstanding any other provision of the Agreement, you may incorporate into your programs or applications, and distribute as incorporated in such programs or applications, the Amazon Athena JDBC Driver or the Amazon Athena ODBC Driver, in each case solely for use with Amazon Athena.

50. AWS Machine Learning and Artificial Intelligence Services

50.1. "AI Services" means, collectively, Amazon Bedrock, Amazon CodeGuru Profiler, Amazon CodeGuru Reviewer, Amazon Titan, Amazon Comprehend, Amazon Comprehend Medical, Amazon DevOps Guru, Amazon Forecast, AWS HealthLake, Amazon Kendra, Amazon Lex, Amazon Lookout for Metrics, Amazon Personalize, Amazon Polly, Amazon Q, Amazon Rekognition, Amazon Textract, Amazon Transcribe, Amazon Transcribe Medical, Amazon Translate, AWS HealthOmics, AWS HealthImaging, AWS HealthScribe, and AWS App Studio. "AI Content" means Your Content that is processed by an AI Service.

50.2. The output that you generate using AI Services is Your Content. Due to the nature of machine learning, output may not be unique across customers and the Services may generate the same or similar results across customers.

50.3. You agree and instruct that for Amazon CodeGuru Profiler, Amazon Comprehend, Amazon Lex, Amazon Polly, Amazon Rekognition, Amazon Textract, Amazon Transcribe, and Amazon Translate: (a) we may use and store AI Content that is processed by each of the foregoing AI Services to develop and improve the applicable AI Service and its underlying technologies; (b) we may use and store AI Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial-intelligence technologies; and (c) solely in connection with the development and improvement described in clauses (a) and (b), we may store such AI Content in an AWS region outside of the AWS region where you are using such AI Service. This Section does not apply to Amazon Comprehend Medical, Amazon Transcribe Medical, AWS HealthScribe, Amazon Comprehend Detect PII or any AI Service that is not listed in the first sentence of this Section 50.3. You may instruct AWS not to use and store AI Content processed by an AI Service to develop and improve that Service or technologies of AWS or its affiliates by configuring an AI services opt-out policy using AWS Organizations. For access to AI Services via AWS Builder ID, you may instruct AWS to

refrain from using and storing AI Content processed by an AI Service to develop and improve that Service or technologies of AWS or its affiliates by using the opt-out mechanism indicated in the applicable service documentation.

50.4. You are responsible for providing legally adequate privacy notices to End Users of your products or services that use any AI Service and obtaining any necessary consent from such End Users for the processing of AI Content and the storage, use, and transfer of AI Content as described under this Section 50, including providing any required notices and obtaining any required verifiable parental consent under the Children's Online Privacy Protection Act (COPPA) or similar laws and obtaining any required consent of individuals appearing in any images or videos processed by an AI Service. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for notifying us in the event that any AI Content stored by an AI Service must be deleted under applicable law. If you use Amazon Lex in connection with websites, programs or other applications that are directed or targeted, in whole or in part, to children under age 13 and subject to COPPA or similar laws you must: (a) provide all required notices and obtain all required verifiable parental consent under COPPA or similar laws; and (b) notify AWS during the Amazon Lex set-up process using the appropriate (i) check box in the AWS console or (ii) Boolean parameter in the applicable Amazon Lex Model Building Service API request or response as specified by the Amazon Lex technical documentation. Amazon Lex does not store or retain voice or text utterance information from websites, programs, or other applications that you identify in accordance with this Section as being directed or targeted, in whole or in part, to children under age 13 and subject to COPPA or similar laws.

50.5. You will not, and will not allow any third-party to, use the AI Services to, directly or indirectly, develop or improve a similar or competing product or service. The foregoing does not apply to Amazon Forecast and Amazon Personalize.

50.6. AI Services are not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious bodily injury or death or cause environmental or property damage. AI Services may be used in connection with supporting healthcare services but are not medical devices and are not intended to be used by themselves for any clinical decision-making or other clinical use. You are responsible for liability that may arise in connection with any such uses.

50.7. Notwithstanding any other provision of the Agreement, you may incorporate into your programs or applications, and distribute as incorporated in such programs or applications, the binary code that we distribute for AI Services with the AWS Mobile SDKs.

50.8. Law Enforcement Use of Amazon Rekognition. Amazon Rekognition's face comparison feature uses machine learning to detect similarities between faces in different images and generate predictions of the likelihood the same person appears in both images; it does not provide definitive identifications of any person. Given the nature of machine learning systems, the following terms apply when Law Enforcement Agencies use Amazon Rekognition's face comparison feature in connection with criminal investigations. "Law Enforcement Agency" means a government entity whose primary purpose and responsibilities are criminal investigation, apprehension and prosecution.

50.8.1. If Amazon Rekognition is used to assist in identifying a person, and actions will be taken based on the identification that could impact that person's civil liberties or equivalent human rights, the decision to take action must be made by an appropriately trained person based on their independent examination of the identification evidence.

50.8.2. Law Enforcement Agencies that use Amazon Rekognition to assist personnel in making decisions that could impact civil liberties or equivalent human rights must ensure such personnel receive appropriate training on responsible use of facial recognition systems, including how to properly operate the system and interpret its results. For an example of how to implement such training, see the Facial Recognition Policy Development Template published by the U.S Department of Justice's Bureau of Justice Assistance.

50.8.3. Amazon Rekognition may not be used for sustained surveillance of a specific person without following an independent review process that is designed to protect civil liberties or equivalent human rights (such as obtaining a court order, warrant, or other authorization), unless the use is to address exigent circumstances involving a threat of death or serious harm to a person.

50.8.4. Law Enforcement Agencies that use Amazon Rekognition for criminal investigations must provide a public disclosure describing their use of facial recognition systems. The method and content of the disclosure is at the reasonable discretion of the agency, but should be easily accessible to the public (such as a posting on a website), describe how the facial recognition system is used, and summarize safeguards in place to prevent violations of civil liberties or equivalent human rights. For examples, see statements and privacy assessments from the FBI and the Facial Recognition Policy Development Template published by the U.S Department of Justice's Bureau of Justice Assistance.

50.9. Amazon Rekognition. The following terms also apply to Amazon Rekognition:

50.9.1. Amazon has implemented a moratorium on use of Amazon Rekognition's face comparison feature by police departments in connection with criminal investigations. This moratorium does not apply to use of Amazon Rekognition's face comparison feature to help identify or locate missing persons.

50.9.2. You agree that if you use Amazon Rekognition's face APIs to analyze, detect, or process faces in images or videos, then you instruct AWS, as your processor, to: (1) generate face vectors and extract other facial attributes on your behalf; (2) store your face vectors in a secure AWS environment; (3) store, delete, and search your face vectors only at your direction or as necessary to maintain or provide Amazon Rekognition or comply with the law or a binding order of a governmental body; and (4) not use your face vectors for any other purpose (unless you instruct otherwise in writing) or transfer them to any third party. As the owner and controller of your face vectors, you instruct us to store them solely within AWS's secure environment.

50.9.3. Your use of Amazon Rekognition is subject to additional Biometric Notice and Consent Service Terms.

50.10. Defense of Claims and Indemnity for Indemnified Generative AI Services. AWS Services may incorporate generative AI features and provide Generative AI Output to you. "Generative AI Output" means output generated by a generative artificial intelligence model in response to inputs or other data provided by you. "Indemnified Generative AI Services" means, collectively, generally available features of Amazon Titan Text Express, Amazon Titan Text Lite, Amazon Titan Text Premier, Amazon Titan Text Embeddings, Amazon Titan Multimodal Embeddings, Amazon Titan Image Generator, AWS HealthScribe, Amazon Personalize, Amazon Q (including Amazon Q Developer Pro in-line code suggestions previously known as Amazon CodeWhisperer Professional, but excluding Amazon Q Developer Free Tier), Amazon Connect Contact Lens, and Amazon Lex. The following terms apply to the Indemnified Generative AI Services:

50.10.1. Subject to the limitations in this Section 50.10, AWS will defend you and your employees, officers, and directors against any third-party claim alleging that the Generative AI Output generated by an Indemnified Generative AI Service infringes or misappropriates that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

50.10.2. AWS will have no obligations or liability under Section 50.10.1 with respect to any claim: (i) arising from Generative AI Output generated in connection with inputs or other data provided by you that, alone or in combination, infringe or misappropriate another party's intellectual property rights; (ii) if you interfere with or fail to enable available filters and other tools, or disregard instructions made available for the Indemnified Generative AI Service; (iii) if your use of the Indemnified Generative AI Service breaches the Agreement; (iv) if you have fine-tuned, refined, customized, or otherwise modified an Indemnified Generative AI Service and the alleged infringement or misappropriation would not have occurred but for this fine-tuning, refinement, customization, or modification; (v) arising after you receive notice to stop using the Generative AI Output; (vi) arising from Generative AI Output that you know or reasonably should know may infringe or misappropriate another party's intellectual property rights; or (vii) alleging that your use of Generative AI Output infringes a third party's trademark or related rights. The remedies in this Section 50.10 are the sole and exclusive remedies under the Agreement for any third-party claims alleging that the Generative AI Output generated by an Indemnified Generative AI Service infringes or misappropriates a third party's intellectual property rights. AWS's defense and payment obligations under this Section 50.10 will not be subject to any damages cap under the Agreement.

50.10.3. The obligations under this Section 50.10 will apply only if you: (a) give AWS prompt written notice of the claim; (b) permit AWS to control the defense of the claim; (c) retain and provide sufficient records to the extent necessary to evaluate your eligibility for the defense of claims and indemnity set forth in this Section 50.10; and (d) reasonably cooperate with AWS (at AWS's expense) in the defense and settlement of the claim. AWS may settle the claim as AWS deems appropriate, provided that AWS obtains your prior written consent (not to be unreasonably withheld) before entering into any settlement.

50.11. Neither you nor your End Users will, or will attempt to, reverse engineer, disassemble, or decompile AI Services, or apply any other process or procedure to derive the source code or other underlying components (such as the model, model parameters, or model weights) or reproduce the training data of AI Services.

50.12. Amazon Bedrock. The following terms apply to Amazon Bedrock:

50.12.1. Third-party models are made available to you as "Third-Party Content" under your Agreement with AWS and are subject to additional third-party license terms specified in Amazon Bedrock and related documentation. Your access to and use of third-party models on Amazon Bedrock may require your use of AWS Marketplace, and in those cases Section 20 (AWS Marketplace) of the Service Terms apply. Notwithstanding anything to the contrary in the Agreement or Service Terms, for purposes of facilitating your purchases of Amazon Bedrock, Amazon Web Services, Inc. will be the AWS Contracting Party.

50.12.2. As part of providing the Service, Amazon Bedrock may use automated abuse detection mechanisms designed to detect harmful content, including related to potential violations of our or third-party model providers' terms of service or acceptable use policies. If these mechanisms detect apparent child sexual abuse material, you agree and instruct that we may report the incident to the National Center for Missing and Exploited Children or other authority. In addition, we may share information, that does not include Your Content, about your use of a third-party model on Amazon Bedrock with the provider of that third-party model. See here for more details.

50.12.3. Provisioned throughput commitments for Bedrock. We may change provisioned throughput commitment pricing or stop offering commitments for provisioned throughput at any time. Any price changes will not apply to existing commitments. Provisioned throughput commitments are nontransferable and noncancellable, so you will be charged for the duration of the term you selected, even if you terminate the Agreement.

50.12.4. Amazon Bedrock may allow you to customize models with data you provide (for example, by fine-tuning). You will have exclusive use of your customized model. Third-party model providers cannot access your customized model. We will not access or use your customized model except as necessary to maintain or provide the Amazon Bedrock Service, or as necessary to comply with the law or a binding order of a governmental body.

50.12.5. Mistral on Bedrock. Any Mistral Models offered on Amazon Bedrock ("Mistral Models") are trained and developed by Mistral AI ("Mistral") and are Third-Party Content. If you use the Mistral Models the following additional terms apply:

- Mistral Models are provided on an "as is" basis and may be modified, updated, or enhanced from time to time.
- AWS may share information with Mistral about your use of the Mistral Models, including Account Information and usage information (but not Your Content), for Mistral's internal business analytics and support of the Mistral Models on Bedrock.
- Mistral owns all right, title, and interest in and to the Mistral Models. You will not have any access to the weights or source code of the Mistral Models without Mistral's consent.
- Subject to the limitations below, Mistral will defend you against any third-party claim alleging that the Mistral Models or output from the Mistral Models infringes or misappropriates that third-party's intellectual property rights.

- Mistral will have no indemnity obligations or liability for any third-party claim arising from: (i) output generated in connection with inputs or other data provided by you that infringe or misappropriate another party's intellectual property rights; (ii) your combination of the Mistral Models with your or a third-party's software or hardware where the claim would not have arisen but for this combination (iii) your interference with or failure to enable available filters and other tools or follow instructions made available for the Mistral Models; (iv) your breach of this section 50.12.5; (v) your fine-tuned, refined, customized, or otherwise modified Mistral Models where the alleged infringement or misappropriation would not have occurred but for this fine-tuning, refinement, customization, or modification; or (v) your failure to comply with applicable law.
- To the extent permitted by applicable law, and except with respect to Mistral's indemnity obligations to you: Mistral will not be liable for any indirect, special, incidental, punitive, exemplary or consequential damages (including real or alleged loss of revenues) or any liabilities, damages and costs incurred by you in the case of: (i) a force majeure event; (ii) any cause not attributable to Mistral; or (iii) output of a Mistral Model being similar or identical to any other customer's output; and for any such claims Mistral's liability to you will be limited to the lower of the aggregate payments you made to AWS for your use of the Mistral Models in the immediately preceding 4 months and EUR 10,000, except for Mistral's open source models where the maximum liability will be the lower of 1 month of payments and EUR 1,000.
- You will defend, indemnify, and hold harmless Mistral, its affiliates, and its licensors from and against any losses arising out of a third-party claim caused by: (a) your use of the Mistral Models in violation of this section 50.12.5; (b) your application (if any); and (c) by any finetuned, refined, customized or modified Mistral Model where the claim would not have arisen but for this fine-tuning, refinement, customization, or modification.

50.12.6. Llama 3, Llama 3.1, and Llama 3.2 on Bedrock. Llama 3, Llama 3.1, and Llama 3.2 are trained and developed by Meta Platforms, Inc. and Meta Platforms Ireland Limited (collectively, **"Meta"**) and is Third-Party Content. If you use Llama 3 on Bedrock then the following additional terms apply: https://llama.meta.com/llama3/license/. If you use Llama 3.1 on Bedrock then the following additional terms apply: https://github.com/meta-llama/llama-models/blob/main/models/llama3_1/LICENSE. If you use Llama 3.2 on Bedrock then the following additional terms apply: https://github.com/meta-llama/llama-models/blob/main/models/llama3_2/LICENSE.

50.12.7. Output generated by models accessed through Amazon Bedrock may include information such as metadata, digital signatures, or watermarks to identify it is generated using a generative artificial intelligence model ("Provenance Data"), as indicated in applicable documentation (for example, see here for Amazon Titan Image Generator). Neither you nor any End User may modify, tamper with, remove, obscure, or otherwise alter such Provenance Data.

50.13. Amazon Q. To help Amazon Q provide the most relevant information, we may use AI Content processed by Amazon Q, such as prompts and responses ("Amazon Q Content"), for service improvement as described below. Currently, this Section 50.13 applies only to Amazon Q Developer Free Tier, but we may add Amazon Q features from time to time as they launch. This Section 50.13 does not apply to Amazon Q Business, Amazon Q Developer Pro, or Amazon Q in AWS Supply Chain.

50.13.1. Service Improvement. You agree and instruct that we may use Amazon Q Content to develop and improve Amazon Q and its underlying technologies, and for that purpose we may store Amazon Q Content in an AWS region outside of the AWS region where you are using Amazon Q.

50.13.2. Other Service Improvement. You agree and instruct that we may also use Amazon Q Content that does not contain personal data to develop and improve AWS and affiliate machine-learning and artificial intelligence technologies including to train machine-learning models.

50.13.3. Further Instructions. You may instruct AWS not to use and store Amazon Q Content for service improvement as described in this Section 50.13 by (i) configuring an AI services opt-out policy using AWS Organizations, (ii) if you use Amazon Q in the IDE, by adjusting your settings in the IDE, or (iii) using the opt-out mechanism described in the Amazon Q documentation.

51. Amazon Lightsail

51.1. You authorize AWS to peer your Amazon Lightsail VPCs and your Amazon VPCs when using Amazon Lightsail VPC peering.

51.2. Amazon Machine Images from the AWS Marketplace are offered or sold under the terms of the AWS Marketplace and any separate terms and conditions and privacy policies specified by the party offering or selling the Amazon Machine Image. Use of Microsoft Software on Amazon Lightsail is subject to Section 5.1 above. Microsoft is an intended third-party beneficiary of this Section 51.2, with the right to enforce its provisions.

51.3. You may not use Amazon Lightsail in a manner intended to avoid incurring data fees from other Services (e.g., proxying network traffic from Services to the public internet or other destinations or excessive data processing through load balancing or content delivery network (CDN) Services as described in the technical documentation), and if you do, we may throttle or suspend your data services or suspend your account.

52. AWS Systems Manager

52.1. Systems Manager may collect and transmit to AWS information regarding your use of the Services, including inventory items (e.g., application inventory and custom inventory items); parameters; configuration data (e.g., network and state configuration); telemetry and diagnostics data; update history and registry keys; resource groups; and patch metadata ("Systems Information"). Systems Information may be used by AWS to improve the Service.

52.2. Certain features of this Service include functionality that allows notifications to be sent to a contact channel (e.g., telephone number, email address). Your use of these features instructs us to send notifications (e.g., SMS/voice messages/emails) to the contact channels entered in the applicable workflows and confirms that you are authorized to send such notifications. Carriers may charge for notifications sent or received in connection with these features.

52.3. Your use of AWS-ApplyChefRecipes is subject to Section 23.2. above.

53. Amazon Chime and Amazon Chime SDK

53.1. In this section, "Amazon Chime" includes Amazon Chime and Amazon Chime SDK.

53.2. End Users.

53.2.1. You may enable End Users to use Amazon Chime under your account. Termination of your account's use of Amazon Chime will also terminate such End Users' paid features, Voice Connector features, and Business Calling features associated with your account or organization, and all such End Users will be converted to the free features of Amazon Chime.

53.2.2. Amazon Chime End Users can be managed by End Users with administrative privileges ("Amazon Chime Administrators"). Amazon Chime Administrators can (a) upgrade or downgrade End Users' Amazon Chime tier and feature set; (b) suspend End User's access to Amazon Chime; and (c) access information about their End Users' use of Amazon Chime, including call details.

53.2.3. Amazon Chime SDK allows developers to integrate communications features into a customer's application. You are responsible for the use of Amazon Chime SDK under your account as part of your application or offering. You are also responsible for the activities of users of such applications or offerings, including their compliance with applicable laws and regulations, the AWS Acceptable Use Policy, and these Terms. AWS may suspend your use of Amazon Chime SDK for non-compliance with such requirements by you or your users.

53.3. Chime PSTN Service.

53.3.1. The term "Chime PSTN Service" as used in these Terms means the ability for you to integrate Public Switched Telephone Network (PSTN) calling and text messaging features into your Amazon Chime experience. The Chime PSTN Service includes (a) dial in access to meetings from the PSTN via standard toll numbers and toll-free numbers; (b) dial out access from meetings to PSTN numbers via standard toll or toll-free numbers; (c) dial in access to Amazon Chime softphones from the PSTN via standard toll or toll-free numbers; (d) dial out access from the Amazon Chime softphone to the PSTN via standard toll or toll-free numbers; (e) receiving text and multi-media messages in Amazon Chime messaging or to APIs via standard toll or toll-free numbers; (f) sending text and multi-media messages from Amazon Chime messaging or from APIs via standard toll or toll-free numbers; (g) dial in access to Amazon Chime Voice Connector from the PSTN via standard toll or toll-free numbers; (h) dial out access from the Amazon Chime Voice Connector to the PSTN via standard toll or toll-free numbers; (i) dial in access to APIs from PSTN via toll or toll-free phone numbers; and (j) dial out access from APIs to the PSTN via standard toll or toll-free numbers.

53.3.2. Portions of the Chime PSTN Service, specifically Business Calling, Voice Connector, and SMS Text, are sold and provided by AMCS LLC ("AMCS"), an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement. Your invoice will state which Services that you have used are sold to you by AMCS and which are sold by AWS. Invoicing for the Chime PSTN Service is performed by AWS on behalf of AMCS for administrative convenience. You do not have to purchase any services sold by AMCS or the Chime PSTN Service to use Amazon Chime, and you may purchase the Chime PSTN Service calling features (such as inbound or outbound calling) separately, together, or not at all from AMCS. AWS is not a telecommunications provider and does not provide any telecommunications-related services.

53.3.3. In using the Chime PSTN Service, you will not: (a) call or text PSTN telephone numbers (whether singly, sequentially, or automatically) to generate income from access or termination charges for you or others as a result of placing the call or texting, (b) engage in unusual calling patterns inconsistent with normal, individual use, or (c) resell the Chime PSTN Service to any third party without our prior written consent.

53.3.4. Your use of the Chime PSTN Service in certain countries are subject to additional Country Specific Communications Service Terms.

53.4. If, as a part of Amazon Chime, AMCS provides you or your End Users with any telephone number (whether toll or toll-free), you understand and agree that you do not own the number and you do not have the right to keep that number indefinitely subject to any number portability rights under applicable law. AMCS reserves the right to change, cancel, or move telephone numbers.

53.5. You and your End Users have the option to use Amazon Chime to record the applicable audio or video session along with chat and other types of recordings (collectively, "Recording"). If you or your End Users request that an audio or video session or other communication be recorded, Amazon Chime will attempt to notify you and your End Users of the Recording by providing a brief audio or visual notice at the time you and your End Users sign in to participate in the applicable session or communication. You and your End Users acknowledge that such notice or attempted notice followed by continued participation in the session or communication constitutes your effective consent to the Recording. You and your End Users understand that use of any Recording may be subject to laws or regulations regarding the recording of telephone calls and other electronic communications, and that it is your and your End Users' responsibility to comply with all applicable laws regarding the Recording, including properly notifying all participants in a recorded session or to a recorded communication that the session or communication is being recorded and obtain their consent. Neither AWS nor its affiliates will be liable for your or your End Users' unlawful Recording, including failure to provide notice or obtain consent. Any notice provided by AWS to alert participants that a session or communication is being recorded may not be relied upon by you or your End Users as definitive disclosure for your or your End Users compliance with applicable laws regarding the Recording.

53.6. Unless stated otherwise, your or your End Users' subscription to any of Amazon Chime's free features does not require the payment of a subscription fee. Amazon Chime's free features are not guaranteed for any period of time, and AWS may restrict, change, limit, or terminate the use of "free" or "basic" features of Amazon Chime by any individual, entity, or group of entities. If you or your End Users sign up for and use paid features of Amazon Chime and then for any reason, including non-payment or breach, your or your End Users' access to the paid services is terminated, you and your End Users may be reverted to the free

features of Amazon Chime and may no longer have access to data and other material that you or your End Users may have stored in connection with Amazon Chime, and that data and material may be deleted by AWS.

53.7. Emergency calling.

53.7.1. The Chime PSTN Service, including Voice Connector features and Business Calling features, is not a traditional telephone service or a replacement for traditional telephone service. Amazon Chime does not provide emergency calling to any emergency services personnel or public safety answering points ("Emergency Services") outside the United States. End Users should not make an Emergency Services call from a location outside the United States because the call will not to be routed to the call answering service for that location.

53.7.2. Within the United States, Voice Connector and Business Calling features support 911 calls to Emergency Services differently than through traditional telephone services. Amazon Chime may not know the physical location of End Users and depends on End Users having access to power and the internet. As calls to Emergency Services in the United States made using Voice Connector or Business Calling features will not automatically provide an End User's location information, the End User must provide their emergency address information to the operator that answers the call. You and your End Users are responsible for ensuring that a valid call-back number is provided with any 911 call placed using Voice Connector or Business Calling. You are solely responsible for any arrangements with third parties to provide your End Users with access to Emergency Services, and AWS makes no representations or warranties regarding the use of any such arrangements with Amazon Chime. You agree to inform your End Users that (a) the Chime PSTN Service cannot be used to make calls if the End User experiences a power outage, cannot access the Internet, or their device has no power, (b) Emergency Services calls in the United States using the Chime PSTN Service may not be routed appropriately because Amazon Chime may not know the End User's location, and (c) End Users may access Emergency Services via other means that may be available to them, including any alternative arrangements that you make available.

53.7.3. The Amazon Chime SDK features do not support calls to Emergency Services. If you permit End Users to place outbound calls or send outbound SMS from a dialpad enabled by Amazon Chime SDK, you must provide prominent notice to your End Users that access to the Emergency Services is not supported.

53.7.4. Neither AWS nor its affiliates are liable for any damages resulting from any Emergency Services call or any inability to place or complete an Emergency Services call using Amazon Chime. AWS disclaims all responsibility for the conduct of local emergency response centers, third parties engaged by you to facilitate emergency response location or other address updates, and all other third parties involved in the provision of Emergency Services. As permitted by applicable law, you agree to release, indemnify, and hold harmless AWS and its affiliates from and against any liability relating to: (a) any acts or omissions of such third parties or other third parties involved in the handling of or response to any emergency call, (b) your inability to use the Chime PSTN Service to contact Emergency Services due to lack of power or internet access; (c) any failure by you or your End Users to provide accurate caller location information or call back information; or (d) your failure to make additional arrangements to access Emergency Services.

53.8. Amazon Chime SDK Machine Learning Services. "Amazon Chime SDK ML Services" means the speaker search and voice tone analysis features of the Amazon Chime SDK. "Amazon Chime SDK ML Content" means Your Content that is processed by an Amazon Chime SDK ML Service. The following terms apply to your use of Amazon Chime SDK ML Services:

(a) You agree and instruct that: (i) we may record, use and store Amazon Chime SDK ML Content to develop and improve Amazon Chime SDK ML Services and their underlying technologies; (ii) we may record, use and store Amazon Chime SDK ML Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial intelligence technologies; and (iii) solely in connection with the development and improvement described in clauses (i) and (ii), Amazon Chime SDK ML Content may be stored in AWS regions outside the AWS regions where you are using Amazon Chime SDK ML Services. You may instruct AWS not to record, use and store Amazon Chime SDK ML Content processed by Amazon Chime SDK ML Services to develop and improve that Service or technologies of AWS or its affiliates by configuring an AI services opt-out policy using AWS Organizations.

(b) You are responsible for providing legally adequate privacy notices to End Users of your products or services that use Amazon Chime SDK ML Services and obtaining any necessary consent from such End Users for the processing of Amazon Chime SDK ML Content and the recording, storage, use, and transfer of Amazon Chime SDK ML Content as described under this Section. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for notifying us in the event that any Amazon Chime SDK ML Content stored using Amazon Chime SDK ML Services must be deleted under applicable law.

(c) You will not, and will not allow any third-party to, use Amazon Chime SDK ML Services to, directly or indirectly, develop or improve a similar or competing product or service.

53.9. Amazon Chime SDK speaker search

53.9.1. Your use of Amazon Chime SDK speaker search is subject to additional Biometric Notice and Consent Service Terms.

53.10. Amazon Chime SDK ML Services use machine learning models that generate predictions based on patterns in data. Output generated by Amazon Chime SDK ML Services is probabilistic and should be evaluated for accuracy as appropriate for your use case, including by employing human review of the output or combining it with other verification factors. You and your End Users are responsible for all decisions made, advice given, actions taken, and failures to take action based on your use of Amazon Chime SDK ML Services.

53.11. Amazon Chime in Japan is sold and provided by AMCS, but is otherwise subject to the terms of the Agreement.

53.12. Amazon Chime in Singapore is sold and provided by AMCS SG PRIVATE LIMITED, an affiliate of AWS, but is otherwise subject to the terms of the Agreement.

53.13. You understand and agree that we store all user information (including chat messages, contacts, calendar, and meeting recordings) in the United States region(s) where the Amazon Chime service is hosted.

53.14. The Chime PSTN Service in the European Economic Area (EEA), the United Kingdom and Switzerland is sold and provided by AMCS, but is otherwise subject to the terms of the Agreement.

54. Amazon Connect

54.1. Connect PSTN Service.

54.1.1. The term "Connect PSTN Service" as used in these Service Terms means the inbound and outbound Public Switched Telephone Network (PSTN) calling features that you may optionally purchase to use with Amazon Connect. The Connect PSTN Service includes dial in access to Amazon Connect from the PSTN via standard toll numbers and toll-free numbers.

54.1.2. The Connect PSTN Service is sold and provided by AMCS LLC ("AMCS"), an affiliate of AWS, and not AWS, but is otherwise subject to the terms of the Agreement. The Connect PSTN Service for Singapore is sold and provided by AMCS SG PRIVATE LIMITED ("AMCS SG"), an affiliate of AWS, and not AWS, but is otherwise subject to the terms of the Agreement. Invoicing for the Connect PSTN Service is performed by AWS on behalf of AMCS and AMCS SG for administrative convenience. You do not have to purchase any service sold by AMCS, AMCS SG, or the Connect PSTN Service to use Amazon Connect, and you may purchase the Connect PSTN Service calling features (such as inbound or outbound calling) separately, together, or not at all from AMCS or AMCS SG. AWS is not a telecommunications provider and does not provide any telecommunications-related services.

54.1.3. In using the Connect PSTN Service, you will not: (a) call PSTN telephone numbers (whether singly, sequentially, or automatically) to generate income from access or termination charges for you or others as a result of placing the call, or (b) engage in unusual calling patterns inconsistent with normal, individual use.

54.1.4. At the customer's request where number portability is available, the applicable AMCS entity will endeavor to transfer telephone numbers that are provided by the AMCS entity or transferred by the customer for use with the Amazon Connect service to a new service provider. However, due to limitations under applicable law and the policies of underlying telecommunications service providers, we may in some cases be unable to transfer a customer's telephone number.

54.1.5. We reserve the right to change or reclaim telephone numbers assigned by the applicable AMCS entity (not including numbers that the customer has ported to Amazon Connect) in the event of a breach of these terms, where necessary for compliance with applicable law or regulation, or if the number has not been used for 90 days.

54.1.6. Your use of the Connect PSTN Service in certain countries are subject to additional Country Specific Communications Service Terms.

54.1.7. Calling to premium rate numbers is supported subject to certain limits. Additional charges may apply to calls to premium rate number above those limits. For more information, please contact Amazon Connect support.

54.2. Emergency calling

54.2.1. The Connect PSTN Service is not a replacement for traditional telephone services. Amazon Connect does not support or carry emergency calling to any emergency services personnel or public safety answering points ("Emergency Services") outside the United States. Your call agents and other End Users that may use Amazon Connect should not make an Emergency Services call from a location outside the United States because the call will not to be routed to the call answering service for that location.

54.2.2. Within the United States, the Connect PSTN Service supports 911 calls to Emergency Services differently than through traditional telephone services. Amazon Connect may not know the physical location of End Users and depends on End Users having access to power and the internet. You and your End Users are responsible for ensuring that current location information and a valid callback number for the End User is available to Amazon Connect for any 911 call placed using the Connect PSTN Service. You agree to inform all call agents and other End Users that may use Amazon Connect that: a) the Connect PSTN Service cannot be used to make calls if the call agent or other End User experiences a power outage, cannot access the Internet, or their device has no power, (b) Emergency Services calls in the United States using the Connect PSTN Service may not be routed appropriately because Amazon Connect may not know the call agent's or other End User's location, and (c) they may access Emergency Services via other means that may be available to them, including any alternative arrangements that you have made available.

54.2.3. Neither AWS nor its affiliates will be liable for any damages resulting from any Emergency Services call or any inability to place an Emergency Services call using Amazon Connect. AWS disclaims all responsibility for the conduct of local emergency response centers, third parties engaged by you to facilitate emergency response location or other address updates, and all other third parties involved in the provision of Emergency Services. As permitted by applicable law, you agree to release, indemnify, and hold harmless AWS and its affiliates from and against any liability relating to: (a) any acts or omissions of such third parties or other third parties involved in the handling of or response to any emergency call, (b) your inability to use the Connect PSTN Service to contact Emergency Services due to lack of power or internet access; (c) any failure by you, your call agents or your other End Users that may use Amazon Connect to provide accurate caller location information or call back information; or (d) your failure to make additional arrangements to access Emergency Services.

54.3. There are important service limitations with Amazon Connect. You must carefully review and comply with the applicable technical documentation at all times, including limitations related to call rates and frequency, automated calling, calls to certain regions, use of caller identification data, and others. If you believe you will exceed any limitations for legitimate reasons, you must contact customer service ahead of time to request applicable exceptions, which we may or may not make in our reasonable discretion. Amazon Connect does not support calls to or from facsimile machines or modems. Any caller identification service provided as a part of Amazon Connect is not guaranteed to function at all times.

54.4. It is your responsibility to use Amazon Connect in compliance with the laws and regulations of the countries where you and your call agents are located, including any regulations governing the use of the internet for voice communications and messaging. In India, you agree that you will not allow your call agents or other End Users located in India to use Amazon Connect to place calls to Indian telephone numbers or otherwise to third parties located in India.

54.5. You and your End Users have the option to request that Amazon Connect record an applicable audio session along with chat and other types of recordings (collectively, "Recording"). You and your End Users understand that the making of or use of any Recording may be subject to laws or regulations regarding the recording of telephone calls and other electronic communications or of communications generally, and that it is your and your End Users' responsibility to comply with all applicable laws regarding any Recording, including properly notifying all participants in a recorded session or to a recorded communication that the session or communication is being recorded and obtain their consent. Neither AWS nor its affiliates will be liable for your or your End Users' unlawful Recording, including failure to provide notice or obtain consent.

54.6. To enable the Apple Business Chat integration with Amazon Connect, you must create an Apple Business Register account and are responsible for reviewing and accepting any applicable Apple terms. You agree that you are solely responsible for your or your End User's use of Apple Business Chat, the content you or your End Users send through Apple Business Chat, and compliance with applicable Apple terms.

54.7. Amazon Connect Machine Learning Services. "Amazon Connect ML Services" means, collectively, Amazon Connect Contact Lens, Amazon Connect Customer Profiles, Amazon Connect outbound campaigns, Amazon Q in Connect, and Amazon Connect Forecasting, Capacity Planning, and Scheduling. "Amazon Connect ML Content" means Your Content that is processed by an Amazon Connect ML Service. The following terms apply to your use of Amazon Connect ML Services:

> (a) You agree and instruct that: (i) we may use and store Amazon Connect ML Content to develop and improve Amazon Connect ML Services and their underlying technologies; (ii) we may use and store Amazon Connect ML Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial intelligence technologies; and (iii) solely in connection with the development and improvement described in clauses (i) and (ii), we may store your Amazon Connect ML Content in AWS regions outside the AWS regions where you are using Amazon Connect ML Services. You may instruct AWS not to use and store Amazon Connect ML Content processed by Amazon Connect ML Services to develop and improve that Service or technologies of AWS or its affiliates by configuring an AI services opt-out policy using AWS Organizations.

(b) You are responsible for providing legally adequate privacy notices to End Users of your products or services that use Amazon Connect ML Services and obtaining any necessary consent from such End Users for the processing of Amazon Connect ML Content and the storage, use, and transfer of Amazon Connect ML Content as described under this Section. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for notifying us in the event that any Amazon Connect ML Content stored by Amazon Connect ML Services must be deleted under applicable law.

(c) You will not, and will not allow any third-party to, use Amazon Connect ML Services to, directly or indirectly, develop or improve a similar or competing product or service.

(d) Amazon Connect ML Services are not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious bodily injury or death or cause environmental or property damage. Amazon Connect ML Services may be used in connection with supporting healthcare services but are not medical devices and are not intended to be used by themselves for any clinical decision-making or other clinical use.

54.8. Amazon Connect Voice ID

54.8.1. Your use of Amazon Connect Voice ID is subject to additional Biometric Notice and Consent Service Terms.

54.8.2. You will not, and will not allow any third-party to, use Amazon Connect Voice ID to, directly or indirectly, develop or improve a similar or competing product or service.

54.8.3. Amazon Connect Voice ID uses machine learning models that generate predictions based on patterns in data. Output generated by Amazon Connect Voice ID is probabilistic and should be evaluated for accuracy as appropriate for your use case, including by employing human review of the output or combining it with other verification factors. You and your End Users are responsible for all decisions made, advice given, actions taken, and failures to take action based on your use of Amazon Connect Voice ID.

54.9. Amazon Connect outbound campaigns. You are responsible for complying with legal requirements related to unsolicited or unwanted communications or telemarketing, including without limitation, the Telephone Consumer Protection Act (TCPA), the FTC's Telemarketing Sales Rule, the EU e-Privacy Directive, UK Privacy and Electronic Communications Regulations, Ofcom's policies regarding nuisance calls and texts, or any similar federal, state, or local laws and regulations. We reserve the right to suspend your use of Amazon Connect outbound campaigns if the percentage of answered calls falls below 20% of calls made in any 7 day period or such other level as we may establish in our documentation or policies for outbound campaigns.

54.10. You may only use Amazon Connect Chat for its intended purpose as set forth in the technical documentation. Other uses, including without limitation creating chats for the primary purpose of sending non-chat-based communications, such as email, are not permitted and may result in additional fees being charged to your account or in any increased service limits being reverted to default capacity.

55. AWS Greengrass

Your use of the AWS Greengrass Core is governed by the AWS Greengrass Core Software License.

56. AWS Migration Hub

When you use AWS Migration Hub, data that is scanned by AWS Migration Hub in your on-premises computing resources will be deemed Your Content.

57. Amazon MQ (AMQ)

If your messages sent through Amazon MQ are blocked, delayed, or prevented from delivery by reasons outside of our control, your payment obligations continue.

58. AWS Media Services

58.1. The distribution of files created by AWS Media Services may require that you obtain license rights from third parties, including owners or licensors of certain third party audio and video formats. You are solely responsible for obtaining such licenses and paying any necessary royalties or fees.

58.2. AWS Elemental MediaConnect and Amazon Interactive Video Service ("IVS") in Japan are sold and provided by AMCS LLC, an affiliate of AWS, and not AWS, but are otherwise subject to the terms of the Agreement.

58.3. AWS Elemental Media Event Management (MEM)

> **58.3.1.** In order to provide MEM, we may request that you implement specific AWS Elemental Software updates and/or provide us with prompt and reasonable access to your AWS Elemental Products. MEM Services do not include installation, configuration, administration, performance, operation, error, fault or defect resolution or other support and maintenance of any AWS Elemental Products, AWS Services or any third-party products (or any combination of any of the foregoing).

58.3.2. AWS does not provide security, risk, governance, legal or compliance advice. You are responsible for making your own assessment of whether your use of the MEM Services meets applicable legal and regulatory requirements. You are also solely responsible for carrying out any advice or recommendations we provide.

58.3.3. Payments for MEM Services are not refundable, and your sole remedy is for AWS to re-perform the relevant MEM Services, provided that you must notify us of any failure within 10 business days of the original date of performance. We will invoice you in the manner set forth on your engagement summary.

58.4. In conjunction with AWS Media Services, you can use watermarking software and technology developed and owned by third-parties (Licensors). This technology is Third-Party Content. You are solely responsible for obtaining all required licenses from Licensors to use their technology, paying any necessary royalties or fees, and complying with applicable terms and conditions.

59. AWS Entity Resolution

59.1. "AWS Entity Resolution Content" means Your Content that is processed by AWS Entity Resolution.

59.2. You agree and instruct that: (a) we may use and store AWS Entity Resolution Content to develop and improve AWS Entity Resolution and its underlying technologies; (b) we may use and store AWS Entity Resolution Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial intelligence technologies; and (c) solely in connection with the development and improvement described in clauses (a) and (b), we may store such AWS Entity Resolution Content in an AWS region outside the AWS region where you are using AWS Entity Resolution. You may instruct AWS not to use and store AWS Entity Resolution Content to develop and improve AWS Entity Resolution and AWS and affiliate machine-learning and artificial intelligence technologies by configuring an AI services opt-out policy using AWS Organizations.

59.3. You are responsible for providing legally adequate privacy notices to End Users of your products or services and obtaining any necessary consent from such End Users for the processing of AWS Entity Resolution Content and the storage, use, and transfer of AWS Entity Resolution Content as described under this Section 59. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for notifying us in the event that any AWS Entity Resolution Content stored by AWS Entity Resolution must be deleted under applicable law.

59.4. You will not, and will not allow any third-party to, use AWS Entity Resolution, directly or indirectly, to develop or improve a similar or competing product or service.

60. Amazon SageMaker

60.1. You are responsible for providing legally adequate privacy notices to End Users of your products or services that use Amazon SageMaker (including End Users in your private workforce when using Amazon SageMaker Ground Truth) and obtaining all necessary consents from such End Users.

60.2. Your use of the NVIDIA Corporation's software, toolkits and drivers is subject to the terms and conditions of the NVIDIA Cloud End User License Agreement.

60.3. Amazon SageMaker is not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious body injury or death or cause environmental or property damage, and you are solely responsible for liability that may arise in connection with any such use.

60.4. When using the public workforce of Amazon SageMaker Ground Truth: (a) you may not provide datasets that contain protected health information, personally identifying information, or other personal data, (b) you may not provide datasets that contain adult content without marking it as containing adult content, and (c) you acknowledge and agree that Your Content provided to the public workforce may be moved outside of the AWS region where you are using Amazon SageMaker Ground Truth.

60.5. Amazon Sagemaker Clarify uses statistical analysis techniques to generate metrics that can be used to evaluate statistical bias in data and machine learning models, and to explain how models generate predictions. The output provided by Amazon SageMaker Clarify is not determinative of the existence or absence of statistical bias, or a comprehensive answer for how a model generates predictions. Such output is not legal advice and should be independently evaluated as appropriate for your use case.

60.6. Amazon SageMaker Edge Manager collects performance and usage metrics and data regarding your use of the Service, including model version, inference and upload times, and diagnostic data. We may use these metrics and data to improve the quality and feature sets of the Services and AWS Content.

60.7. We may change SageMaker Savings Plan ("SM Savings Plan") pricing or terminate the program at any time. Any price changes will not apply to previously purchased SM Savings Plans. All amounts paid in connection with SM Savings Plans are nonrefundable, except that if we terminate the Agreement other than for cause, or terminate the SM Savings Plan program, we will refund you a pro rata portion of any up-front fee paid. SM Savings Plans are nontransferable and noncancellable, so you will be charged for the duration of the term you selected, even if you terminate the Agreement. Upon expiration or termination of the term of SM Savings Plans, the reserved pricing will expire and standard on-demand usage prices will apply. You are responsible for determining if you are subject to any limitations arising from the purchase or use of the SM Savings Plan and for complying with any applicable laws, policies, terms or conditions governing your payment of up-front fees, including any fiscal or appropriation laws, or other policies or restrictions governing up-front payments for goods or services.

60.8. Amazon SageMaker Studio Lab

60.8.1. You acknowledge that we may store your Content that is processed by Amazon SageMaker Studio Lab in AWS regions outside the AWS region where you are using Amazon SageMaker Studio Lab.

60.8.2. Amazon SageMaker Studio Lab is provided for training and educational purposes and is not intended for production workloads. AWS may modify your ability to access or use Amazon SageMaker Studio Lab at any time, including any usage or resource limits. Access to Amazon SageMaker Studio Lab features and compute resources, including CPUs and GPUs, are not guaranteed.

60.8.3. If during the previous 3 months you have registered no usage of your Amazon SageMaker Studio Lab account, we may delete your Amazon SageMaker Studio Lab account and any associated Content upon 30 days prior notice to you. Deleting your Amazon SageMaker Studio Lab account permanently and automatically deletes the information associated with your account and any associated Content.

60.8.4. For purposes of your use of Amazon SageMaker Studio Lab, Amazon Web Services, Inc. is the AWS Contracting Party under the Agreement.

61. AWS AppSync

You agree not to and will not attempt to perform any network discovery or load testing of Your Content inside AWS AppSync unless expressly authorized by us in writing.

62. AWS Telco Network Builder

AWS Support. You will remain enrolled in Business Support or better during the entire period of your use of AWS Telco Network Builder.

63. AWS RoboMaker

63.1. AWS RoboMaker includes an integrated development and simulation environment and related assets and tools we make available here (collectively, "RoboMaker Materials").

63.2. In addition to the rights granted to AWS Content under the Intellectual Property License, AWS, Inc. also grants you a limited, revocable, non-exclusive, non-sublicensable (except to End Users as provided below), non-transferrable license to do the following during the Term:

(a) You may use, reproduce, modify, and create derivative works of the RoboMaker Materials to develop and support AWS RoboMaker test and simulation environments that run only on your AWS or your on-premises computing resources (each such simulation environment, a "RoboMaker Simulation").

(b) You may use, reproduce, modify, create derivative works of, publicly display, publicly perform, and distribute to End Users the RoboMaker Materials (including any permitted modifications and derivatives) as part of a RoboMaker Simulation.

(c) You may sublicense the rights set forth in this Section 63.2 to your End Users solely for the purpose of enabling your End Users to use and modify your RoboMaker Simulation.

63.3. Each RoboMaker Simulation must provide material content or functionality beyond that provided by the RoboMaker Materials, and the RoboMaker Materials may not be distributed to End Users except as part of a RoboMaker Simulation.

64. Amazon FSx

64.1. Amazon FSx for Windows File Server. Use of Microsoft Software on Amazon FSx for Windows File Server is subject to Section 5.1 above. Microsoft is an intended third-party beneficiary of this Section 64.1, with the right to enforce its provisions.

64.2. Amazon FSx for NetApp ONTAP. AWS may share Account Information, logs or other usage information with NetApp to enable NetApp to provide technical and sales support.

65. AWS Security Assurance Services

65.1. "AWS Security Assurance Services" are advisory and consulting services that AWS provides under a statement of work ("SOW") to help you run regulated data workloads using other Services. AWS Security Assurance Services are provided by AWS Security Assurance Services LLC ("SAS") or certain of its affiliates. SAS is an affiliate of AWS. AWS Security Assurances Services are "Services" for the purposes of the Agreement.

65.2. SAS or any of its affiliates may enter into a SOW with you to provide AWS Security Assurance Services. For the purposes of each SOW, the term "SAS" in the SOW and the term "AWS" or "SAS" in the Agreement refer only to the SAS entity that executes the SOW, and no other AWS or SAS entity has any obligations under such SOW. Each SOW (together with the Agreement as amended by such SOW) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement and supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to the subject matter of that SOW.

65.3. SAS, or one of its affiliates on behalf of SAS, will invoice you monthly for the AWS Security Assurances Services. Payments for AWS Security Assurances Services are not refundable.

65.4. SAS does not provide legal advice. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

65.5. Other than Third Party Content, Content that SAS provides as part of the AWS Security Assurance Services is AWS Content. You are solely responsible for testing, deploying, maintaining and supporting Content provided or recommended by SAS.

65.6. SAS may develop Content consisting of either (a) documents and diagrams ("Documents") or (b) software (in source or object code form), sample code, or scripts ("Software") for you as part of the AWS Security Assurance Services (such Documents and Software, "Developed Content"). Subject to any non-disclosure agreement in effect between you and SAS, SAS is not precluded from developing, using, or selling products or services that are similar to or related to the Developed Content. Any Developed Content provided to you by SAS as part of the AWS Security Assurance Services under a SOW is licensed under the following terms:

SAS licenses any Documents to you under the Creative Commons Attribution 4.0 International License (CC-BY 4.0); and

SAS licenses any Software to you under the Apache License, Version 2.0.

65.7. Some Developed Content may include AWS Content or Third Party Content provided under a separate license. In the event of a conflict between Section 65.6 above and any separate license, the separate license will control with respect to such AWS Content or Third Party Content.

65.8. Any materials or information that you own or license from a third party and provide to SAS for the purposes of the AWS Security Assurance Services are Your Content.

66. Amazon WorkLink

66.1. You and your End Users may only use the Amazon WorkLink client software on devices owned or controlled by you or your End Users and solely to access Your Content for internal business purposes. Each End User may be permitted to use a limited number of devices or sessions in any calendar month.

66.2. As part of regular operations, Amazon WorkLink may access your End Users' devices that are provisioned as part of the Amazon WorkLink setup to perform configurations, health checks, and diagnostics on a regular basis. During the performance of these tasks, Amazon WorkLink will only retrieve

performance, log data, and other information related to the operation and management of the Service.

67. AWS Training

67.1. "AWS Training" equips individual learners and enterprises with the skills to use, build, and innovate using the cloud, and includes instructor-led training, self-paced digital training, hands-on labs, enterprise training deployment, and other learning content and sessions provided by AWS. Specific categories of AWS Training such as instructor-led classes ("Classroom Training"), self-paced digital training ("Digital Training"), and training deployment support ("Enterprise Skills Transformation" or "EST"), are detailed in sections below. References to "AWS" in any order for AWS Training (an "Order") mean: (a) the applicable AWS Contracting Party as defined in the Agreement, or (b) for Classroom Training provided in certain jurisdictions, the local AWS Contracting Party listed in the Special Provisions for Certain Jurisdictions.

67.2. Payment

67.2.1 Prepayment. Prepayment for enterprise AWS Training is available in those countries listed on the AWS Site. Digital Training Team Subscriptions and EST are not eligible for prepayment. If you opt to prepay, you agree to pay the amount listed in your Order and applicable taxes ("Prepaid Funds") within 30 days of (a) the effective date of your Order, or (b) receipt of the prepayment invoice, whichever is later. If you do not prepay within 30-days, you will pay as described in the Agreement. Prepaid Funds are non-refundable and expire at the end of the term in the applicable Order.

67.2.2. Fees. AWS will charge you a fee equal to the value of any funding, discounts, or credits you receive for enterprise AWS Training if you do not consume AWS Training equal to the total amount listed in your Order, within the term specified in your Order.

67.3. Classroom Training

67.3.1. Individual Classroom Training. To access Classroom Training as an individual, you must create an AWS Training account as directed on the AWS Site, and register for a public class. Once you have registered, AWS will provide you with instructions on how to access the class, the course materials, and any lab environment. You may withdraw from a class by visiting your AWS Training account and withdrawing from the class in your transcript. If a refund is available, you will be informed at the time of withdrawal.

67.3.2. Enterprise Classroom Training. Either you or AWS may request to reschedule or cancel an enterprise Classroom Training class at least 14 days before the class start date. If you request to reschedule or cancel a class less than 14 days before the class start date, AWS may bill you the fee listed in your Order for the canceled class excluding discounts, credits or other funding, incurred travel expenses listed in your Order, and applicable taxes. If you make a timely rescheduling request but AWS is unable to reschedule, you may keep the original class start date, or AWS will cancel the class at no

charge. If AWS makes a timely rescheduling request but you are unable to reschedule, AWS will cancel the class at no charge. The maximum number of individuals you may enroll in an enterprise Classroom Training class is 25.

67.3.2.1. Vouchers. Vouchers for Classroom Training are non-refundable, non-transferable, and may not be resold, licensed, rented, or redeemed for cash. Vouchers must be used before the expiration date listed in your Order, and AWS will bill you for unused vouchers after the vouchers expire. AWS reserves the right to invalidate or reject any voucher without issuing any refund if AWS suspects that it was obtained, used, or applied fraudulently, unlawfully, or otherwise in violation of this Section. As of the date the vouchers are emailed to the contact address listed in the Order, you are solely responsible for any voucher that is lost, stolen, or used without your permission. You may distribute vouchers only to learners who are your employees, affiliates' employees, or contractors who are aware of, and comply with, the restrictions described in this Section.

67.4. Digital Training

67.4.1. Access and Fees. Subscribers to Digital Training on the AWS Site may access and participate in self-paced trainings on the AWS Site an unlimited number of times during their subscription. From time to time, we may add or remove Digital Trainings from the AWS Site and we make no guarantee as to the availability of specific Digital Trainings or the minimum number of Digital Trainings available. If your subscription ends, you will no longer have access to the Digital Trainings you selected from the AWS Site. The service fees for Digital Training subscriptions are stated on the AWS Site. From time to time, we may offer different subscription lengths, and the subscription service fees may vary. Subscription service fees may be subject to tax and are non-refundable except as expressly set forth in this section.

67.4.2. Individual Subscription. You may cancel your individual subscription by visiting your account and adjusting your subscription settings. If you cancel your individual subscription, you will not receive a refund of any subscription fees already paid and the subscription will remain active until the end of the current pay period. You may not transfer or assign your subscription or any Digital Training benefits.

67.4.3. Team Subscription. For an Order of 5 or more subscriptions (“Seats”) to Digital Training on the AWS Site (a “Team Subscription”), you must provide AWS all reasonably necessary setup information within 5 business days of your Order’s effective date, or as otherwise specified in your Order. The Team Subscription provides you access to your Seats on the date AWS gives your learning administrator(s) access for the period listed in your Order. If you inform your AWS training representative in writing within 2 business days of the start date that you do not have access to your Seats, your Team Subscription will not start until AWS confirms you have access. Seats may only be used by a single person for the entire term of the Team Subscription, except that you may reassign up to twenty percent of Seats within your organization during the term of the Team Subscription.

67.4.3.1. Additional Seats. You may purchase additional Seats under your existing Team Subscription by contacting your AWS Training representative as described on the AWS Training detail page on the AWS Site. Your start date for additional Seats begins when AWS gives your

learning administrator(s) access, and any additional Seats purchased will expire at the end of your existing Team Subscription. Fees for additional Seats are calculated pro-rata based on the time remaining in your existing Team Subscription.

67.4.4. Auto-Renewal. Unless you notify us before a charge that you want to cancel or do not want to auto renew, your Digital Training subscription will automatically continue and you authorize us (without notice to you, unless required by applicable law) to collect the then-applicable subscription service fees and any taxes, using any payment method we have on record for you. We may change the Digital Training subscription service fee from time to time by notifying you of the change and effective date before it takes effect. You may reject the change by cancelling your subscription at no additional cost at any time before a subscription service fee change takes effect. From time to time we may also offer non-recurring subscriptions. The provisions in this section regarding automatic renewal are not applicable to those subscriptions.
If all payment methods we have on file for you are declined for payment of your subscription service fees, your subscription will be cancelled unless you provide us with a new payment method. If you provide us with a new payment method that is successfully charged before your subscription is cancelled, your new subscription period will be based on the original renewal date and not the date of the successful charge.

67.5. Enterprise Skills Transformation

67.5.1. Access. To enable EST support and guidance, AWS may require access to your internal communication systems including but not limited to email, instant messaging, and other systems related to such access as identified by you ("Customer Systems"). When accessing Customer Systems, AWS agrees to comply with your reasonable policies and procedures, to the extent such policies and procedures are (i) applicable to such access and use, and (ii) do not conflict with the Agreement. Subject to your prior approval, you will arrange for AWS to have reasonable access to your Customer Systems to the extent required to enable EST, and at no additional cost to AWS. You may revoke your access approval at any time. AWS is not responsible for any failure to perform caused by your revocation of AWS' access to your Customer Systems.

67.5.2. Cancellation. Either you or AWS may cancel your EST engagement with 15 days written notice, which may be via email. AWS will charge you for the full month during which the cancellation takes effect.

68. AWS Certification

"AWS Certification Program" means the program through which AWS makes available professional certifications and other credentials in connection with the Services. The AWS Certification Program is a "Service" for purposes of the Agreement. To participate in the AWS Certification Program, you must agree to the Certification Program Agreement ("CPA"). To the extent there is a conflict between the Agreement and the CPA, the CPA controls.

69. Migration Evaluator

Migration Evaluator collects performance and usage metrics and data about your virtual machine image(s) and IT infrastructure; software packages and applications; system, equipment, and application configuration, processes and performance; network configurations, communications and dependencies; and the installation and operation of Migration Evaluator and its components. We may use these metrics and data to provide, maintain, and improve the quality and feature sets of the Services and AWS Content.

70. AWS IQ

70.1. AWS IQ Experts ("Providers") offer their services ("Provider Services") as independent contractors, and are not employees of you or us. AWS is not a party to the agreement between you and any Providers for their Provider Services, is not responsible or liable for Provider Services, and does not guarantee the quality or accuracy of Provider Services. For avoidance of doubt, any certification that a Provider obtains from us only certifies that the Provider has passed a test intended to evaluate the Provider's proficiency and understanding of a particular AWS Service or area of knowledge to which that certification relates, and is not a guarantee that the Provider Services will be performed at any particular level of quality, speed, or to your specific requirements.

70.2. AWS charges service fees for transactions between you and Providers on the AWS IQ marketplace. AWS only collects these service fees if you and a Provider pay and receive payment through the AWS IQ marketplace. Therefore, for 24 months from the time you identify a Provider through AWS IQ, you agree to use AWS IQ as your exclusive method to pay for Provider Services. For avoidance of doubt, if you did not identify a Provider through use of AWS IQ, such as if you worked with a Provider prior to connecting with that Provider on AWS IQ, then this section does not apply.

70.3. You acknowledge and agree that we may use information from AWS IQ listings, proposals, chat communications, and additional terms proposed or agreed to between you and Providers on AWS IQ to develop and improve the quality and feature set of AWS IQ.

70.4. If you choose to grant Providers access to your AWS account, you are solely responsible and liable for (a) any actions taken by the Provider in your account; (b) the Provider's use of Your Content or use of the Services or AWS Content; (c) ensuring the Provider complies with your obligations under the Agreement, the Acceptable Use Policy, any other Policies, the Intellectual Property License and applicable laws; (d) ensuring the Provider does not use the Services or AWS Content in any manner or for any purpose other than as expressly permitted by the Agreement and the Intellectual Property License; and (e) ensuring Provider does not attempt to (i) modify, distribute, alter, tamper with, repair, or otherwise create derivative works of any AWS Content or other Content included in the Services (except to the extent Content included in the Services is provided to you under a separate license that expressly permits the creation of derivative works), (ii) reverse engineer, disassemble, or decompile the Services or AWS Content or apply any other process or procedure to derive the source code of any software included in the Services or AWS Content (except to the extent applicable law doesn't allow this restriction), (iii) access or use the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (iv) resell or sublicense the Services or AWS Content. You will

immediately revoke Provider's access to your AWS account if you become aware of any violation of your obligations under the Agreement or the Intellectual Property License caused by a Provider with access to your AWS account. If you use AWS IQ's feature that allows you to grant a Provider access to your account, AWS may, but is not obligated to, review activities in your account for security purposes, and may revoke the Provider's access at any time.

70.5. You release us (and our agents and employees) from claims, demands, and damages (actual or consequential) of any and every kind and nature, known or unknown, suspected or unsuspected, disclosed and undisclosed, arising out of or in any way connected with your use of the AWS IQ marketplace.

71. AWS Cloud WAN

71.1. AWS Cloud WAN in Japan is sold and provided by AMCS LLC, an affiliate of AWS, and not AWS, but is otherwise subject to the terms of the Agreement.

71.2. AWS Cloud WAN in Singapore is sold and provided by AMCS SG PRIVATE LIMITED, an affiliate of AWS, and not AWS, but is otherwise subject to the terms of the Agreement.

71.3. Your use of AWS Cloud WAN in South Korea is subject to the applicable Country Specific Communications Service Terms.

72. AWS CodeStar Notifications

AWS CodeStar Notifications utilizes one or more of the following: Amazon Simple Notification Service (Amazon SNS), Amazon Simple Email Service (SES), and/or AWS Chatbot. If utilized, your use of AWS CodeStar Notifications is also subject to the terms that govern those Services.

73. AWS Data Exchange

73.1. The Service Terms for AWS Marketplace Sellers apply to your use of AWS Data Exchange. Your use of Content obtained through AWS Data Exchange remains subject to the AWS Acceptable Use Policy, even if used outside of our Services.

73.2. You may not use any Content obtained through AWS Data Exchange that was anonymized, de-identified, or otherwise disassociated from an identifiable person in any manner that would attempt to re-identify, de-anonymize, or otherwise associate such Content with an identifiable person.

73.3. If we remove your Data Offering (as defined in the Service Terms for AWS Marketplace Sellers), then we may also cancel any current associated subscriptions if we determine, in our sole discretion, that your Data Offering: (a) poses a security risk to us or a Subscriber (as defined in the Service Terms for

AWS Marketplace Sellers); (b) could subject us, our affiliates, or any third party to liability; (c) could be fraudulent; or (d) violates the AWS Marketplace Service Terms.

73.4. Except as agreed to in writing between you and the respective Subscriber, otherwise permitted by law, in addition to any other restrictions on your use of Subscriber Information (as defined in the Service Terms for AWS Marketplace Sellers) in the Service Terms for AWS Marketplace Sellers, you may only use Subscriber Information for compliance verification in connection with Subscribers acquiring rights to the underlying content of your Data Offerings.

73.5. You represent and warrant to us that to the extent your Data Offerings contains any data that (i) identifies or can be used by a Subscriber or other third party to identify a natural person; or (ii) otherwise may be deemed to be personal data or personal information under applicable laws or regulations with respect to the Subscriber, then such data (a) has already lawfully been made available to the general public, such as via governmental records, widely distributed media, or legally required public disclosures; and (b) does not include sensitive data or sensitive information about an individual or shall not otherwise be deemed to be sensitive data or sensitive information under applicable laws and regulations, including without limitation, information relating to biometric or genetic data, health, racial or ethnic origin, political opinions, religious or philosophical beliefs, sex or sexual orientation, trade union membership, or personal payment or sensitive personal data.

73.6. If you do not specify license rights for your Data Offerings, you agree to license your Data Offerings under the terms of the template Data Subscription Agreement available at https://aws.amazon.com/marketplace/features/standardized-contracts.

73.7. Your use of AWS Data Exchange is subject to the fees described in the AWS Data Exchange User Guide.

74. AWS End of Support Migration Program for Windows Server

74.1. The AWS End of Support Migration Program (EMP) for Windows Server Service, including any tools provided for the EMP Service (which are AWS Content), may be used solely for the purpose of migrating Your applications or other Content to Amazon EC2 or other AWS Services.

74.2. You acknowledge that the EMP Service is designed to migrate your applications and other Content to AWS Services and you may not use the EMP Service, including any tools provided for the EMP Service, for ongoing use outside of the AWS Services (e.g., on your on-premises systems), except that you may temporarily run your applications or other Content on your on-premises systems utilizing the EMP Service for up to 30 days to verify functionality prior to migration.

74.3. You consent to the collection and provision of the data collected by the EMP Service and its associated software and components, including information about your virtual machine image(s); software packages; system, equipment, and application configuration, processes and performance; network

configurations, communications and dependencies; relationships between the foregoing; and information about the installation and operation of the EMP Service and its associated software and components ("Migration Information"). Migration Information may be used to improve the quality and feature set of the Services.

75. Amazon Fraud Detector

75.1. AWS is not a consumer reporting agency as defined by the Fair Credit Reporting Act, 15 U.S.C. §1681 et seq. ("FCRA"), or the equivalent under similar laws, and Amazon Fraud Detector does not include or provide "consumer reports" as defined in the FCRA. You may not use Amazon Fraud Detector to determine any person's financial status, financial history, creditworthiness, or eligibility for insurance, housing, or employment.

75.2. You will not, and will not allow any third-party to, use Amazon Fraud Detector to, directly or indirectly, develop or improve a similar or competing product or service.

75.3. You agree and instruct that: (a) we may use, and store Your Content that is processed with Amazon Fraud Detector ("Fraud Detector Content") to develop and improve the Service and its underlying technologies; (b) we may use and store Fraud Detector Content that is not personal data to develop and improve other AWS fraud prevention services; and (c) solely in connection with the usage and storage described in clauses (a) and (b), we may store such Content in an AWS region outside of the AWS region where you are using Amazon Fraud Detector. By following a process we provide you, you may instruct AWS not to use or store Your Content processed by Amazon Fraud Detector to develop and improve Amazon Fraud Detector or other AWS fraud prevention services.

76. Amazon Augmented AI

76.1. You are responsible for providing legally adequate privacy notices to End Users of your products or services that use Amazon Augmented AI (including End Users in your private workforce) and obtaining all necessary consents from such End Users. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents.

76.2. When using the Amazon Mechanical Turk workforce of Amazon Augmented AI: (a) you may not provide data or content that contains protected health information or other information that is identifiable to a specific person, and (b) you acknowledge and agree that Your Content provided to the Amazon Mechanical Turk workforce may be moved outside of the AWS region where you are using Amazon Augmented AI.

76.3. When using the third party vendor workforce option of Amazon Augmented AI, you are responsible for ensuring that the vendor meets any compliance requirements applicable to any personal data or confidential information in your data or content. You may not share data or content that contains protected health information with the third party vendor workforce.

77. AWS Private Certificate Authority

77.1. AWS Private Certificate Authority Connector for SCEP (Preview). When you use AWS Private CA Connector for SCEP (Preview) with Microsoft Intune, certain functionalities are enabled by accessing Microsoft Intune through Microsoft APIs. Your use of the AWS Private CA Connector for SCEP and accompanying AWS Services does not remove your need to have a valid license for your use of the Microsoft Intune service.

78. Wavelength Zones/Local Zones

For the Service Level Agreements applicable to any Services or Service workloads that you run in Wavelength Zones or Local Zones, Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for the individual Service that runs in the affected Wavelength Zones or Local Zones, respectively, for the monthly billing cycle in which the unavailability occurred.

79. Amazon Braket

79.1. If you use Amazon Braket to access quantum computing hardware operated by one of the third-party hardware providers listed here (each a "Hardware Provider"), you: (1) acknowledge that the Content you provide in connection with your use of Amazon Braket may be processed by the Hardware Provider outside of facilities operated by AWS; and (2) authorize AWS to transfer such Content to the Hardware Provider for processing.

79.2. We may change, deprecate or discontinue any Service offering that relates to services offered by any Hardware Provider at any time. We will provide you with prior notice of any deprecation or discontinuation of such a service offering where practicable under the circumstances.

80. Amazon Elastic Container Registry Public

80.1. Amazon Elastic Container Registry Public (Amazon ECR Public) is a public registry that allows you to upload and share Content that anyone with or without an AWS account ("Registry Users") can download and use. In order for you to upload and share Content through Amazon ECR Public, you must grant AWS and Registry Users a license to the Content in accordance with Sections 80.2 and 80.3 below.

80.2. By uploading Content to Amazon ECR Public, you hereby grant AWS and its Affiliates a worldwide, non-exclusive, fully paid-up, royalty-free license to store, parse, copy, reproduce (including by making mechanical reproductions), reformat, transmit, display, and perform the Content in connection with providing Amazon ECR Public, and, with respect to any Third-Party Content you upload that is subject to an open source or Third-Party Content license, you represent and warrant that the terms for such Third-Party Content permit AWS and its Affiliates to store, parse, copy, reproduce (including by making mechanical reproductions), reformat, transmit, display, and perform the Content in connection with providing Amazon ECR Public.

80.3. You may specify the terms under which you license Your Content to Registry Users. If you do not specify such terms when you upload Your Content, you hereby grant to any other Registry User a non-exclusive license to access, download, use, modify or otherwise exploit Your Content for any personal or business purposes. If you upload and share any Third-Party Content to Amazon ECR Public, you are responsible for ensuring that you have the rights and licenses necessary to do so.

81. Industrial AI Services

81.1. "Industrial AI Services" means, collectively, Amazon Lookout for Vision, Amazon Lookout for Equipment, Amazon Monitron, and AWS Panorama. "Industrial AI Content" means Your Content that is processed by an Industrial AI Service.

81.2. Industrial AI Services use machine learning models that generate predictions based on patterns in data. Output generated by a machine learning model is probabilistic and should be evaluated for accuracy as appropriate for your use case, including by employing human review of such output. Output provided by Amazon Lookout for Equipment and Amazon Monitron should not be used as a substitute for regular, scheduled maintenance on machinery and equipment. You and your End Users are responsible for all decisions made, advice given, actions taken, and failures to take action based on your use of Industrial AI Services.

81.3. You agree and instruct that for Amazon Lookout for Vision, Amazon Lookout for Equipment and Amazon Monitron: (a) we may use and store Industrial AI Content that is processed by each of the foregoing Industrial AI Services to develop and improve the applicable Industrial AI Service and its underlying technologies; (b) we may use and store Industrial AI Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial-intelligence technologies; and (c) solely in connection with the development and improvement described in clauses (a) and (b), we may store such Industrial AI Content in an AWS region outside of the AWS region where you are using such Industrial AI Service. You may instruct AWS not to use and store Industrial AI Content processed by an Industrial AI Service to develop and improve that Service or technologies of AWS or its affiliates by (i) for Amazon Monitron, contacting AWS Support and following the process provided to you, and (ii) for Amazon Lookout for Vision and Amazon Lookout for Equipment, by configuring an AI services opt-out policy using AWS Organizations.

81.4. You are responsible for providing legally adequate privacy notices to End Users of your products or services that use any Industrial AI Service and obtaining any necessary consent from such End Users for the processing of Industrial AI Content and the storage, use, and transfer of Industrial AI Content as described under this Section.

81.5. You will not, and will not allow any third-party to, use Industrial AI Services to, directly or indirectly, develop or improve a similar or competing product or service. The foregoing does not apply to AWS Panorama to the extent you are developing hardware appliances that integrate with AWS Panorama, to Amazon Lookout for Equipment, or to Amazon Monitron.

81.6. Industrial AI Services are not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious bodily injury or death or cause environmental or property damage, and you are solely responsible for liability that may arise in connection with any such use.

81.7. Notwithstanding any other provision of the Agreement, you may incorporate into your programs or applications, and distribute as incorporated in such programs or applications, the binary code that we distribute for Industrial AI Services with the AWS Mobile SDKs.

82. Amazon Location Service

82.1. When you use a feature of Amazon Location Service that is identified to you as being provided by a third-party geolocation service provider listed here (each such feature, including Maps, Places, and Routing, a "**Geolocation Provider Feature**," and each such provider, a "**Geolocation Provider**"), you authorize AWS to transmit your request parameters (e.g., location searches) to the Geolocation Provider for processing which may be outside of the AWS region in which your request was made. However, any Open Data requests will be processed by AWS in the AWS region in which your request was made.

82.2. Location Data provided through Amazon Location Service should be evaluated for accuracy as appropriate for your use case. You are responsible for making your own assessment of whether your use of Amazon Location Service meets applicable legal and regulatory requirements. You and your End Users are solely responsible for all decisions made, advice given, actions taken, and failures to take action based on your use of Amazon Location Service.

82.3. AWS may change, deprecate, or discontinue any Geolocation Provider or Geolocation Provider Feature at any time upon notice to you. We will provide you with prior notice of any deprecation or discontinuation of a Geolocation Provider or Geolocation Provider Feature where practicable under the circumstances.

82.4. For Geolocation Providers other than Open Data, you may not:

a. Scrape, systematically collect, duplicate, store, or cache the data provided to you from Amazon Location Service (e.g., map tiles, forward and reverse geocodes, routes, drive times/isochrones, and other data) (collectively, "Location Data"), including for the purpose of avoiding use of Amazon Location Service, except that you may store or cache:

(i) route results for up to 30 days when you use HERE or Esri as your Geolocation Provider (other than as prohibited in Section 82.5.a),

(ii) geocoding and reverse-geocoding results (other than as prohibited in Section 82.5.a) when you indicate the result will be stored in the API parameter, or

(iii) any Location Data to comply with legal or regulatory requirements.

b. Use Location Data to create or offer a product or service with features that are similar to the services of the Geolocation Providers, where such product or service does not contain substantial, independent value and features beyond the services of the Geolocation Providers.

c. Incorporate Amazon Location Service, including any Location Data, into any integrated in-vehicle infotainment system, any systems for autonomous control of the vehicle, or any real-time dynamic routing or route optimization applications installed on in-vehicle hardware. In-vehicle mobile device applications, including ones mirroring onto a vehicle's onboard display system, are permitted.

d. Use, incorporate, modify, distribute, provide access to, or combine any Location Data in a manner that would subject the Location Data to open-source or open-database license terms that require any part of the Location Data to be disclosed to third parties, licensed to third parties for the purpose of making derivative works, or redistributed to third parties at no charge.

e. Use Location Data to develop paper maps or an atlas (digital or otherwise) for purposes of sale or distribution to others.

f. Place your company name or marks, or any third-party advertisements, on or in the Location Data (e.g., on a map display).

82.5. In addition to the restrictions in Section 82.4, if you use HERE as your Geolocation Provider, you may not:

a. Store or cache any Location Data for Japan, including any geocoding or reverse-geocoding results.

b. Layer routes from HERE on top of a map from another third-party provider, or layer routes from another third-party provider on top of maps from HERE.

82.6. In addition to the restrictions in Section 82.4, if you use Esri as your Geolocation Provider, you may not, without our express written consent, use any of its Geolocation Provider Features for asset management or asset tracking use cases (i.e., to locate, track, or route any vehicles, cargo, personnel, or other assets that you use in your business).

82.7. You may not use Amazon Location Service for any hazardous, unsafe, or illegal activities, including any use in, or association with, any hazardous environments or critical systems that may lead to serious bodily injury or death or cause environmental or property damage. You are solely responsible for all liability that may arise in connection with any such use.

82.8. We may suspend or terminate your access to, or limit your use of, Amazon Location Service immediately upon notice to you, if we reasonably determine you are using Amazon Location Service in violation of our terms, including in any manner intended to avoid incurring appropriate usage fees or in violation of applicable law or order of a governmental body.

82.9. Open Data uses OpenStreetMap data. OpenStreetMap is licensed under the Open Data Commons Open Database License (ODbL) by the OpenStreetMap Foundation. You agree to comply with the ODbL and acknowledge the attribution and share-alike provisions therein.

82.10. Attribution for Location Data can be found here. You must pass through attribution for Location Data that you make available to others via your application or its product documentation. If any Location Data has attribution details attached or incorporated, you may not remove, modify, or obscure (or permit any End Users to remove, modify, or obscure) any copyright, trademark notice, restrictive legend, or other proprietary right notices supplied to you.

83. AWS Managed Services

83.1. If you request that AWS Managed Services be provided for any software or service that is not expressly identified as supported in the AWS Managed Services user guides posted on the AWS Site ("Customer-Requested Configuration"), any AWS Managed Services provided for such Customer-Requested Configuration will be treated as a "Beta Service" under these Service Terms.

83.2. You represent and warrant to AWS that the person requesting any of your AWS accounts to be an AWS Managed Services Account (as defined in the AWS Managed Services user guides posted on the AWS Site) is authorized to make such requests and procure AWS Managed Services on your behalf and with respect to such AWS accounts.

83.3. AWS and its affiliates will not be liable to you for any damages arising from (a) AWS's actions taken pursuant to any instructions or requests that you provide or approve, (b) you not following an instruction or recommendation from AWS, (c) your delay or withholding of approval for AWS to take a requested action, or (d) any change by you to your Managed Environment (as defined in the AWS Managed Services user guides posted on the AWS Site).

84. Amazon FinSpace

Amazon FinSpace is a tool to help you analyze data for investment and business decisions. It is not a substitute for the judgment and experience of the user when making investment and business decisions. Amazon FinSpace does not provide investment advice, make investment recommendations or evaluate the suitability of any investment or investment strategy.

85. Amazon Elastic Kubernetes Service Anywhere (Amazon EKS Anywhere) Support

85.1. You must purchase AWS Enterprise Support in order to subscribe to Amazon EKS Anywhere Support. Payments for subscriptions to Amazon EKS Anywhere Support are not refundable.

85.2. Each Amazon EKS Anywhere Support Subscription may only be applied to one Amazon EKS Anywhere cluster.

85.3. We may request that you implement specific updates and provide us with Account Information, logs or other usage information so that we can provide you Amazon EKS Anywhere Support and verify your Support Subscription. If you request support for Isovalent's software, such as Cilium, we may share your Account Information, logs or other usage information with Isovalent to provide technical support.

86. AWS DeepRacer Student

86.1. You acknowledge that we may store your Content that is processed by AWS DeepRacer Student in AWS regions outside the AWS region where you are using AWS DeepRacer Student.

86.2. If you participate in AWS DeepRacer Student competitions or related activities (including preseason exhibitions), AWS may publicly share your username, avatar, and performance results, such as via leaderboards, blog posts, and social media.

86.3. AWS DeepRacer Student is provided for training and educational purposes and is not intended for production workloads. AWS may modify your ability to access or use AWS DeepRacer Student at any time, including any usage or resource limits. Access to AWS DeepRacer Student features and compute resources, including CPUs and GPUs, are not guaranteed.

86.4. If during the previous 12 months you have registered no usage of your AWS DeepRacer Student account, we may delete your AWS DeepRacer Student account and any associated Content upon 30 days prior notice to you. Deleting your AWS DeepRacer Student account permanently and automatically deletes the information associated with your account and any associated Content.

86.5. For purposes of your use of AWS DeepRacer Student, Amazon Web Services, Inc. is the AWS Contracting Party under the Agreement.

86.6. You must be a student in high school or a higher education institution, and at least 16 years old, to use AWS DeepRacer Student. If you are under 18 years of age, or the age of majority in your location, you may use AWS DeepRacer Student only with involvement of a parent or guardian who agrees to be bound by these Service Terms.

87. Amazon GuardDuty

87.1. “Malware Content” is Your Content that the Amazon GuardDuty Malware Protection feature processes and identifies as being malicious or harmful.

87.2. You agree and instruct that: (a) we may use and store Malware Content to develop and improve Amazon GuardDuty and its underlying technologies; (b) we may use and store Malware Content that is not personal data to develop and improve other AWS security services; and (c) solely in connection with the development and improvement described in clauses (a) and (b), we may store such Malware Content in an AWS region outside the AWS region where you are using the Amazon GuardDuty Malware Protection feature. You may instruct AWS not to use and store Malware Content to develop and improve Amazon GuardDuty or other AWS security services by configuring an AI services opt-out policy using AWS Organizations.

87.3. “Runtime Monitoring Content” means Your Content that is processed by the Amazon GuardDuty Runtime Monitoring feature.

87.4. You agree and instruct that: (a) we may use and store Runtime Monitoring Content to develop and improve Amazon GuardDuty and its underlying technologies; and (b) we may use and store Runtime Monitoring Content that is not personal data to develop and improve other AWS security services. You may instruct AWS not to use and store Runtime Monitoring Content to develop and improve Amazon GuardDuty or other AWS security services by configuring an AI services opt-out policy using AWS Organizations.

88. AWS Wickr

88.1. End Users.

> **88.1.1.** You may enable End Users to use AWS Wickr under your account. Termination of your account’s use of AWS Wickr may also suspend or terminate such End Users’ features or access associated with your account or organization.
>
> **88.1.2.** AWS Wickr End Users can be managed by End Users with administrative privileges (“AWS Wickr Administrators”). AWS Wickr Administrators can (a) upgrade or downgrade End Users’ AWS Wickr feature set; (b) suspend End User’s access to AWS Wickr; and (c) access information about their End Users’ use of AWS Wickr.

89. AWS Private 5G

89.1. AWS Private 5G Equipment. AWS will make equipment available to you to support your use of the AWS Private 5G Service (the “Private 5G Equipment”). AWS, or its affiliates, maintain all rights in the Private 5G Equipment and is not selling, renting, leasing, or transferring any ownership, intellectual or other rights in the Private 5G Equipment to you. You will not, and will not purport to, assign, grant, or transfer the Private 5G Equipment or any interest in the Private 5G Equipment to any individual or entity, and any such purported assignment, grant or transfer is void.

89.2. Facility Assessment. You will ensure that, at all times, the facility at which the Private 5G Equipment is located (the "Designated Facility") meets the minimum requirements necessary to support the installation, maintenance, use, and removal of the Private 5G Equipment as described here and otherwise as described in the AWS Private 5G technical documentation or provided to you during the ordering process. When moving the Private 5G Equipment from the Designated Facility to a new Designated Facility, you must notify AWS of the new Designated Facility's Address.

89.3. Delivery. You will ensure that you have all necessary rights, certifications, and licenses for the delivery, installation, maintenance, use, and removal of the Private 5G Equipment at the Designated Facility.

89.4. Use. You are responsible for the installation, use, and removal of the AWS Private 5G Equipment at the Designated Facility and returning the Private 5G Equipment to AWS as described in the AWS Private 5G technical documentation or provided to you during the ordering process. Except as provided for in the technical documentation, you will ensure that no one accesses or repairs the Private 5G Equipment. In addition to other rights and remedies AWS may have under the Agreement, AWS may charge a lost device fee if the Private 5G Equipment is lost or damaged between when it is first in your possession and when the carrier accepts the Private 5G Equipment for delivery back to AWS. AWS may terminate your use of AWS Private 5G and remove the Private 5G Equipment if you breach these terms or materially breach the terms of the Agreement with respect to AWS Private 5G. In the event that we terminate your use of AWS Private 5G and remove the Private 5G Equipment in accordance with this Section 89.4, we will provide you with prior notice where practicable under the circumstances.

89.5. Business Support. You will remain enrolled in AWS Support at the Business level during the entire period of your use of AWS Private 5G.

89.6. Security. As the Private 5G Equipment is physically located at the Designated Facility, you are responsible for physical security and access controls, as well as all power, networking, and environmental conditions at your Designated Facility. Consequently, any AWS commitments in the Agreement that depend on AWS's operation of such physical security and access controls, or power, networking, and environmental conditions, do not apply to AWS Private 5G.

90. AWS SimSpace

90.1. We may change, discontinue, or deprecate support for any third-party integrations or samples at any time. We will provide you with prior notice of any deprecation or discontinuation of support for a third-party integration or sample where practicable under the circumstances.

90.2. AWS SimSpace Weaver is designed to help customers build simulations. This may include simulation of real-world locations, scenarios, and assets, based on the simulation code and data you provide. Data generated by AWS SimSpace Weaver should be evaluated for accuracy as appropriate for your use case. You and your End Users are solely responsible for all decisions made, advice given, actions taken, and failures to act based on your use of AWS SimSpace Weaver.

91. AWS Builder ID

91.1. If during the previous 12 months you have registered no usage of your AWS Builder ID, we may delete your AWS Builder ID upon 30 days' prior notice.

91.2. Upon deletion of your AWS Builder ID, you will no longer have access to Your Content through your AWS Builder ID, and such content will be deleted.

91.3. For purposes of your use of AWS Builder ID, Amazon Web Services, Inc. is the AWS Contracting Party under the Agreement.

92. AWS Clean Rooms

92.1. You may not use AWS Clean Rooms or any information obtained from your use of AWS Clean Rooms to identify a person or associate such information with an identifiable person, unless otherwise permitted by the applicable third-party contributor of the data.

92.2. AWS Clean Rooms may provide you with the ability to collaborate (an "AWS Clean Rooms Collaboration") with other AWS customers (an "Other AWS Customer"). You may make available Your Content, including a dataset and/or a custom model, as part of an AWS Clean Rooms Collaboration. You may also disclose Your Content to, or receive Third-Party Content from an Other AWS Customer.

92.3. If you request deletion of Your Content from the AWS Clean Rooms Collaboration dataset, or if an Other AWS Customer that is a participant to the AWS Clean Rooms Collaboration requests deletion of its Third-Party Content from the AWS Clean Rooms Collaboration dataset, we will delete all Your Content and all Third-Party Content from the AWS Clean Rooms Collaboration dataset.

92.4. Any interaction as part of an AWS Clean Rooms Collaboration will be governed by separate terms and conditions between you and such Other AWS Customer (if any).

92.5. AWS Clean Rooms ML

92.5.1. You will not, and will not allow any third-party to, use AWS Clean Rooms ML to, directly or indirectly, develop or improve a similar or competing product or service to AWS Clean Rooms ML.

92.5.2. AWS Clean Rooms ML is not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious bodily injury or death or cause environmental or property damage. AWS Clean Rooms ML may be used in connection with supporting

healthcare services but is not a medical device and is not intended to be used by itself for any clinical decision-making or other clinical use. You are responsible for liability that may arise in connection with any such uses.

93. Amazon CodeCatalyst

93.1. When you access an Amazon CodeCatalyst Space established under another CodeCatalyst account ("Third-Party Space"), you are an End User of that CodeCatalyst account. This means, for example, that your activities within the Third-Party Space may incur fees for which that Third-Party Space owner is responsible. Additionally, Content you contribute to a Third-Party Space or Project within that Space ("Contributed Content") as an End User is not considered Your Content for the purposes of rights and obligations under the terms of this Agreement. Subject to the non-exclusive license granted by Section 93.2, this does not modify any rights you may hold in your Contributed Content.

93.2. Contributed Content, including issues, comments, and contributions to a Third-Party Space, may be viewed by others who have access to that Third-Party Space. Unless you enter into a license with other parties who have access to the Third-Party Space specifying different terms, you grant each party who has access to the Third-Party Space a nonexclusive, worldwide, irrevocable license to use, reproduce, prepare derivatives, distribute, perform, and display Contributed Content. You represent and warrant that you have all rights necessary to grant this license.

93.3. When you invite another CodeCatalyst account owner to collaborate in your Space, they become an End User of your CodeCatalyst account and their Contributed Content is considered Your Content under the terms of the Agreement. You are responsible for the conduct of End Users that you invite to collaborate, including their Contributed Content, and for maintaining all End User permissions for purposes of data security and access. You are responsible for all fees you and End Users may accrue for using CodeCatalyst or any affiliated Service in connection with your Space.

93.4. Unless you delegate administrative permissions over your CodeCatalyst Space to another CodeCatalyst account owner, you agree that termination of your CodeCatalyst account or deletion of any of Your Content or Contributed Content in your Space, whether by you or by us, may also terminate your End Users' access to Your Content and Contributed Content in your Space. In order to access billable services within or in connection with your CodeCatalyst account, you must link an AWS account. If you delete your CodeCatalyst account but have delegated administrative permissions to another CodeCatalyst account owner, your AWS account will continue to be billed for the billable services unless you also un-link your AWS account.

93.5. When an End User you have invited to collaborate in your CodeCatalyst Space deletes their CodeCatalyst account, their Contributed Content will not be deleted from your Space. However, identifications of that End User, including those associated with issues, comments, and Contributed Content, may be deleted.

94. Integrated Private Wireless on AWS

94.1. AWS may stop providing the Integrated Private Wireless on AWS portal (or remove any offerings on the Integrated Private Wireless on AWS site (or any successor site)) at any time. We will provide you with prior notice where practicable under the circumstances.

94.2. The offerings on the Integrated Private Wireless on AWS site (or any successor site) are offered by third parties and subject to separate terms and conditions specified by the respective third party. AWS has no control and makes no guarantees about such offerings.

95. AWS Diode

95.1. AWS Diode allows You to map Your account to another Diode account ("Mapped Account"), enabling Your Content to be moved and stored by the Mapped Account to an AWS region of a different classification level. You acknowledge and agree that using the Service may result in Your Content being moved and stored in AWS regions other than the AWS regions where You initially stored Your Content.

95.2. You are responsible for all data transferred through AWS Diode, including, but not limited to: (i) compliance with all laws, regulations, and policies related to the control, disclosure, and transfer of classified information; and (ii) transferring data only to AWS regions of appropriate classification levels. Your failure to do so may result in Amazon incurring sanitization costs for which You will be responsible, and which will be exempt from any limitations of liability in any of your agreements with AWS.

96. AWS Nitro System

AWS personnel do not have access to Your Content on AWS Nitro System EC2 instances. There are no technical means or APIs available to AWS personnel to read, copy, extract, modify, or otherwise access Your Content on an AWS Nitro System EC2 instance or encrypted-EBS volume attached to an AWS Nitro System EC2 instance. Access to AWS Nitro System EC2 instance APIs – which enable AWS personnel to operate the system without access to Your Content - is always logged, and always requires authentication and authorization.

97. Amazon Security Lake

97.1. "Security Lake Content" is Your Content that (a) Amazon Security Lake processes or (b) is stored in Amazon Security Lake.

97.2. You agree and instruct that: (a) we may use and store your Security Lake Content to develop and improve Amazon Security Lake and its underlying technologies; and (b) we may use and store Security Lake Content that is not personal data to develop and improve other AWS security services. You may instruct AWS not to use and store Security Lake Content to develop and improve Amazon Security Lake or other AWS security services by configuring an AI services opt-out policy using AWS Organizations.

98. Amazon Managed Blockchain

You are solely responsible for evaluating the information made available through the Amazon Managed Blockchain Query Service for accuracy as appropriate for your use case.

99. Amazon DataZone

99.1. DataZone generates probable forecasts, insights or recommendations from Your Content, and its outputs should be evaluated for accuracy as appropriate for your use case, including by employing human review of such output. You and your End Users are responsible for all decisions made, advice given, actions taken, and failures to take action.

99.2. Amazon DataZone Machine Learning Services. "Amazon DataZone ML Services" means DataZone Automatic Business Name Generation and AI Recommendations for Descriptions in DataZone. "Amazon DataZone ML Content" means Your Content that is processed by an Amazon DataZone ML Service. The following terms apply to your use of Amazon DataZone ML Services:

a. You agree and instruct that: (i) we may use and store Amazon DataZone ML Content to develop and improve Amazon DataZone ML Services and their underlying technologies; (ii) we may use and store Amazon DataZone ML Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial intelligence technologies; and (iii) solely in connection with the development and improvement described in clauses (i) and (ii), we may store your Amazon DataZone ML Content in AWS regions outside the AWS regions where you are using Amazon DataZone ML Services. You may instruct AWS not to use and store Amazon DataZone ML Content processed by Amazon DataZone to develop and improve that Service or technologies of AWS or its affiliates by configuring an AI services opt-out policy using AWS Organizations.

b. You are responsible for providing legally adequate privacy notices to End Users of your products or services that use Amazon DataZone ML Services and obtaining any necessary consent from such End Users for the processing of Amazon DataZone ML Content and the storage, use, and transfer of Amazon DataZone ML Content as described under this Section. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for notifying us in the event that any Amazon DataZone ML Content stored by Amazon DataZone ML Services must be deleted under applicable law.

100. AWS re:Post Private

100.1. You acknowledge that we may store Your Content that is processed by AWS re:Post Private in AWS regions outside the AWS region where you are using AWS re:Post Private.

100.2. Use of AWS re:Post Private is subject to the Terms of Use for AWS re:Post Private which are available in your private re:Post.

101. Amazon One Enterprise

101.1. Amazon One Enterprise Services (Preview). "Amazon One Enterprise Service" includes all Services and Amazon Content AWS or its affiliates provide in conjunction with Amazon One Enterprise Devices. "Amazon One Enterprise Devices" are the hardware and equipment Amazon One Enterprise makes available to you to support your use of the Amazon One Enterprise Service. You understand and agree that the Amazon One Enterprise Service is intended for use only in the commercial or business context and that you will not use the Amazon One Enterprise Service in any way to collect information or provide services to your End Users in their personal or household capacity

101.2. Facility Requirements. You will ensure that, at all times, the facility at which Amazon One Enterprise Devices are installed and located ("Facility") meets any requirements necessary to support the installation, maintenance, use, and removal of Amazon One Enterprise Devices as described in any Amazon One Enterprise Devices technical documentation or indicated to you during the ordering and installation process. You are responsible for any damage to Amazon One Enterprise Devices at the Facility. The Amazon One Enterprise Device Terms of Use govern your purchase and use of Amazon One Enterprise Devices.

101.3. Access to Amazon One Enterprise Devices. You will give personnel designated by AWS prompt and reasonable access to the Facility as necessary to deliver, install, service, repair, or inspect Amazon One Enterprise Devices. You will not require AWS personnel to sign, accept, or otherwise agree to any terms, conditions, obligations, or agreements of any kind as a condition of accessing the Facility, and you agree that the terms of any such documentation are void even if signed by AWS personnel or its designees. You will ensure that no one modifies, alters, reverse engineers, repairs, or tampers with Amazon One Enterprise Devices. You acknowledge that Amazon One Enterprise Devices may be equipped with tamper monitoring technology.

101.4. Palm Data. You agree and instruct that to provide the Amazon One Enterprise Services, AWS will generate, analyze, process, store, and use data related to your End Users' palms, including palm images, palm signatures, embeddings, and representations ("Palm Data") on your behalf when you make the Amazon One Enterprise Device available for use to your End Users. AWS will generate, analyze, process, store, and use Palm Data only as necessary to maintain and provide the Amazon One Enterprise Service or as necessary to comply with applicable laws or a binding order of a governmental body, and to develop and improve the Amazon One and Amazon One Enterprise Services. AWS will not sell Palm Data or use Palm Data in cross-context behavioral advertising. Palm Data include, but are not limited to, unique images, templates, and/or mathematical representations of End Users' palms that are created using proprietary software and algorithms. Palm Data are integral to the functioning of the Amazon One Enterprise Services and AWS generates, analyzes, processes, stores, uses, and makes available Palm Data on your behalf solely for use in the Amazon One Enterprise Services. You understand and agree that Palm Data, and all related information, technology, processing and outputs required to generate, analyze, process, store, and use Palm Data, are not Your Content (as defined by the Agreement). You understand that all forms of Palm Data: (i) have economic value for AWS; (ii) are not readily known or knowable to others and; (iii) are subject to AWS's reasonable efforts to keep them secret and confidential, and are, therefore, a trade secret of AWS and owned by AWS. You understand and

agree that you and your End Users will not have any access to Palm Data, and you agree to notify your End Users of this before they use any Amazon One Enterprise Device.

101.5. Your use of Amazon One Enterprise Services is subject to additional Biometric Notice and Consent Service Terms.

101.6. Privacy Rights Requests. You are solely responsible for receiving submissions for and responding to any requests from your End Users or individuals you authorize or permit to use the Amazon One Enterprise Services relating to their personal information (collectively, "Privacy Rights Request") in compliance with applicable laws. To the extent AWS receives any Privacy Rights Requests, AWS will forward such Privacy Rights Requests to you and reasonably cooperate in providing you the necessary information for you to comply with Privacy Rights Requests. Further, you understand and agree that to the extent any Privacy Rights Requests relate to Palm Data, after you have verified the identity of the requestor: (a) if the request is a deletion request, you will notify AWS of the request, and AWS will permanently destroy the Palm Data in accordance with applicable law; or (b) if the request is an access or portability request, you will inform the requestor with sufficient particularity that you have collected Palm Data, but you understand and agree that you will not be able to disclose or provide access to Palm Data because it is sensitive personal information and applicable privacy laws prohibit you from disclosing or providing access to such sensitive personal information in response to a Privacy Rights Request. Moreover, you understand and agree that you do not and will not have access to Palm Data because it constitutes both sensitive personal information and AWS's trade secret.

101.7. Notwithstanding anything to the contrary, you agree and instruct that we may analyze, process, use, and store Your Content, End User information to: (a) maintain and provide Amazon One Enterprise Services, and (b) develop and improve Amazon One and Amazon One Enterprise Services, including any underlying technologies and any training and testing machine learning models. Except as expressly provided herein, you acknowledge and agree that you and your End Users will not have any rights, title, or interest in any Amazon products or services or AWS Content and that we may process and store Your Content and End User information in AWS regions outside the AWS regions where you are using Amazon One Enterprise.

101.8. You will not, and will not allow any third-party to use Amazon One Enterprise Services to, directly or indirectly, develop or improve a similar or competing product or service.

102. Amazon WorkSpaces Thin Client

In addition to the Agreement and these Service Terms, use of Amazon WorkSpaces Thin Client devices is subject to device terms. Please review the device terms before using an Amazon WorkSpaces Thin Client device.

103. AWS Deadline Cloud

103.1. When you use AWS Deadline Cloud, you have the option to license digital content creation software ("**DCC Software**") from separate third-party providers. DCC Software is Third-Party Content. If you elect to use DCC Software, you agree that AWS is not a party to any agreement between you and any DCC Software provider governing your use of the DCC Software, AWS is not responsible or liable to you for the DCC Software, and AWS does not make any representations or warranties with respect to the DCC Software. The following additional terms and conditions apply to use of DCC Software:

a. Your use of Foundry's Software is subject to the terms and conditions of the Foundry End User License Agreement.

b. Your use of Side Effects Software Inc.'s Software is subject to the terms and conditions of the Side Effects Software License Agreement.

c. Your use of Autodesk's Software is subject to the terms and conditions of the Autodesk License and Services Agreement, the Autodesk Terms of Use, and the Autodesk Additional Terms.

d. Your use of Autodesk's Arnold for Maya is subject to the terms and conditions of the End User License Agreement which is installed on the worker in the Arnold EULA folder.

e. Your use of Blender Foundation's Software is subject to the terms and conditions of the GNU General Public License.

f. Your use of Luxion's Keyshot is subject to the terms and conditions of the Terms and Conditions.

103.2. AWS does not offer support services for DCC Software. You may request support directly from the applicable DCC Software provider, who may require your agreement with additional terms and conditions, including privacy notices. AWS is not responsible for any support provided by third-party DCC Software providers, and makes no guarantees about such services.

103.3. AWS may change, deprecate, or discontinue any offering of DCC Software at any time upon notice to you. We will provide you with prior notice of any deprecation or discontinuation of DCC Software where practicable under the circumstances.

103.4. AWS Deadline Cloud is not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious body injury or death or cause environmental or property damage, and you are solely responsible for liability that may arise in connection with any such use.

Previous version(s)

Learn About AWS

- What Is AWS?
- What Is Cloud Computing?
- AWS Accessibility
- AWS Inclusion, Diversity & Equity
- What Is DevOps?
- What Is a Container?
- What Is a Data Lake?
- What is Artificial Intelligence (AI)?
- What is Generative AI?
- What is Machine Learning (ML)?
- AWS Cloud Security
- What's New
- Blogs
- Press Releases

Resources for AWS

- Getting Started
- Training and Certification
- AWS Solutions Library
- Architecture Center
- Product and Technical FAQs
- Analyst Reports
- AWS Partners

Developers on AWS

- Developer Center
- SDKs & Tools
- .NET on AWS
- Python on AWS
- Java on AWS
- PHP on AWS
- JavaScript on AWS

Help

- Contact Us
- Get Expert Help
- File a Support Ticket
- AWS re:Post
- Knowledge Center
- AWS Support Overview
- Legal
- AWS Careers

Amazon is an Equal Opportunity Employer: *Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.*

Language

عربي |
Bahasa Indonesia |
Deutsch |
English |
Español |
Français |
Italiano |
Português |
Tiếng Việt |
Türkçe |
Русский |
ไทย |
日本語 |
한국어 |
中文 (简体) |
中文 (繁體)