



STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 2

CONTRACT #: AR2489

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Smartronix, LLC (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

The attached pricing and rate schedule is amended as an additional document into the Attachment C: Pricing Discounts and Pricing Schedule.

The current Attachment E cloud service provider T&Cs are fully replaced with the attached Attachment E cloud service provider T&Cs.

Effective Date of Amendment: as of the last signature date below.

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

STATE OF UTAH

Melinda Armsworthy

5/1/2020

Contractor's Signature

Date

May 7, 2020

Director, State of Utah Division of Purchasing

Date

Melinda Armsworthy
Contractor's Name (Print)

Director of Contracts
Title (Print)

For Division of Purchasing Internal Use

Purchasing Agent	Phone #	E-mail Address	Contract #
Solomon Kingston	801-957-7142	skingston@utah.gov	AR2489

NASPO Product Schedule (with Pricing Notes and Explanations)

The attached Product Schedule offers pricing for the following Cloud Models: IaaS, PaaS, and SaaS. Smartronix is offering our Cloud Assured Managed Services (CAMS) for cloud services utilized in Public and Government Community Clouds.

The prices for Public and Government Community Cloud Services can be found in this Product Schedule and receive a 3% discount off commercial list prices. The pricing and discount schedule for Smartronix Managed Services is also contained within this Product Schedule.

Due to the rapid innovation and growth of available services in the cloud marketplace, Smartronix is offering the use of all current and future cloud services as they are available. Complete information on the suite of products available to NASPO Participating Entities under contract with Smartronix can be found in the following links:

- AWS: <https://aws.amazon.com/products>
- Azure: <https://azure.microsoft.com/en-us/services/>
- GCP: <https://cloud.google.com/products/>

Note: Not all services are available in all regions.

Current commercial list pricing for all services can be found here:

- AWS: <https://aws.amazon.com/pricing/services/>
- Azure: <https://azure.microsoft.com/en-us/pricing/>
- GCP: <https://cloud.google.com/pricing/>

Pricing Methodology

Smartronix' pricing and discounts are based on consumption (or utility style), with Managed Services costs broken out from the cost of compute. We believe separating the cloud services from the management costs provide the customer with the most flexibility and transparency.

First we are offering discounts, outlined below, based on monthly Cloud Services Provider (CSP) consumption. For example, utilizing cloud reporting tools, we run determine consumption cost for CSP services at list price. We then discount that amount and invoice the Participating Entity. Many of the services from our Cloud Assured Managed Services (CAMS) offering, invoiced separately from your cloud services, are priced per instance. In a variable environment where instances are stood up and shut down frequently, the number of effective instances are invoiced, determined by the calculation below:

$$\frac{\text{Total hours consumed}}{\text{Total hours in that month}} = \# \text{ of effective instances}$$

Cloud Services Price Estimating

The CSPs that Smartronix represents provide pricing calculators to estimate the cost of their services. These calculators are an important tool to estimate the cost of future task orders. With all prices being

publicly available, there are no hidden cost. These calculator for each CSP can be found at these locations:

- AWS: <http://calculator.s3.amazonaws.com/index.html>
- Azure: <https://azure.microsoft.com/en-us/pricing/#explore-cost>
- GCP: <https://cloud.google.com/products/calculator/>

Smartronix Professional Services Rate Card

Labor Category	Hourly Rate
Sr Cloud Architect	\$250
Cloud Architect	\$225
Sr Cloud Engineer	\$200
Cloud Engineer	\$180
Sr Solutions Architect	\$275
Principle/ Managing Consultant	\$290
Cloud Subject Matter Expert	\$300
Security Architect	\$200
Security Analyst	\$175
Sr I&O Engineer	\$140
I&O Engineer	\$120
Cloud Program Manager	\$220
Cloud Project Manager	\$200
CSP Consulting/Professional Services – daily rate	\$3250/day

Smartronix Cloud Assured Managed Services (CAMS) Pricing

Please see Managed Services Catalog (included below as Attachment A) for full details on the managed services provided by Smartronix.

Core Managed Services

Account Services

Service Title	Monthly Price
Account Management Service	\$2000/Account
SLA Management	
Event Management & Incident Response	
Boundary Management	
Log Aggregation (Basic)	
Infrastructure Provisioning Service	\$50/Provisioning Request

Instance Managed Services

Service Title	Monthly Price
Monitoring and Notification	\$300/instance
Operating System Patch Management	
Anti-malware Management	
Backup and Restoration Service	

Cluster Managed Services

Service Title	Monthly Price
Container Service Monitoring and Notification	\$300/cluster
Container Service Patch Management	

**CAMS has a monthly minimum commitment of \$10,000 per month across account, core, and cluster managed services.*

Optional Services

Service Title	Price
Cloud Service Expense Management Advisory Service	1.5% of Invoice monthly
Infrastructure Advisory Services	Priced based on scope
Disaster Recovery Service	Price based on request
Advanced Application Monitoring	Priced based on scope
Enhanced Data Encryption	Price based on request
Application Management Services	Price based on request
Database Management Services	\$400 / instance
Web Management Services and CDN	\$400/ per site distribution
Workspaces Management Services	Tier per Workspace Instance Fee \$25 Per less than 150 Instances \$22 for 150 through 300 \$18 for 300 through 700 \$14 Greater than 700
Serverless Environment – Compliance, Logging, and Real-time monitoring	\$1,000 per application or service mesh

Optional Security Services

Service Title	Price
Security Incident Response	Priced based on scope.
Enhanced Log Aggregation and Analysis	Log Monitoring and Analysis - \$320/per GB of indexed data, based on average daily consumption in a calendar month.
Host Intrusion Detection/Prevention	\$55 per instance
Host File Integrity Monitoring	\$65 per instance
Smartronix CyberHunter	Based on blocks of 400 collections per day \$6,200 per month
Security Systems Vulnerability Scanning	\$300 per instance

Security & Regulatory Compliance Advisory Service	Professional Services Priced based on scope
--	---

*ELAA has a monthly minimal commitment of \$8,000 per month or the total of cost based on average GB indexed per day in a one-month measurement period (based on calendar), whichever is higher.

Notes:

- Customized service/pricing for customer environments that have reduced requirements, e.g. Development, Test, Quality Assurance, User Acceptance Test, or Labs is available.
- CAMS is deployed to customer CSP accounts via Terraform infrastructure as code templates. This enables Smartronix to expedite customer onboarding and ensures quality through a templated, tested, and automated workflow.
- Clients are required to enable Config, CloudTrail, CloudWatch, network flow logs, and allow Smartronix to install AWS CloudWatch agent, AWS SSM agent, and AWS Inspector Agent on managed instances in regions that run services supported by Smartronix.
- Smartronix CAMS will leverage a centralized IdP with MFA enabled login to gain access to the customer CSP account. All actions performed in the customer CSP account will be logged and retained in the customer account for audit purposes.
- Micro services (AWS lambda) will execute service automation tasks within the account to enable instance monitoring, snapshots/backups, and creation of alarms to create event notifications.
- Smartronix will reserve one resource tag for use in the management of the resources.

Discounting

CSP Resale Discounts

Smartronix offers the following discounts off the commercial list price at the time of consumption:

- 3% on Amazon Web Services (AWS)
- 3% on Microsoft Azure
- 3% on Google Cloud Platform (GCP)

Note: There are no discounts provided on products and services sold thru any CSP for which Smartronix does not receive a discount. This currently includes fees associated with: Amazon DevPay, Amazon Mechanical Turk, Amazon Flexible Payment Services and any 3rd party products purchased in the AWS Marketplace.

Smartronix Cloud Assured Managed Services (CAMS) Discounts

The following volume discounts are available on a tiered basis from monthly managed service spend as follows:

Monthly Cost	Vol Discount %
\$0 - \$15,000	0%
\$15,000 - \$30,000	2.5%

\$30,000 - \$45,000	5%
\$45,000 - \$60,000	10%
Over \$60,000	12.5%

Note: These discounts are tiered and are applied based upon monthly managed services spend and are granted and calculated at each tier.

Notes

Amazon Web Services

Note 1: AWS pricing is based on per second consumption.

Note 2: AWS Compute services vary between regional availability and OS

Note 3: When a sufficient number of Reserved Instances in an AWS Region have been purchased, Participating Entities will automatically receive discounts on upfront fees and hourly fees for future purchases of Reserved Instances in that AWS Region. Reserved Instance discounts are determined based on the total list price (non-discounted price) of upfront fees for the active Reserved Instances purchased per AWS Region to determine the applicable volume discount tier. The following is a discounting example considering the following volume discount tiers:

- \$0-\$500K: Upfront - 0%, Hourly - 0%
- \$500K - \$4M: Upfront - 5%, Hourly - 5%
- \$4M - \$10M: Upfront - 10%, Hourly - 10%
- \$10M+: Negotiated

Microsoft Azure

Note 1: Azure pricing is based on per hour consumption.

Note 2: Azure Compute services vary between regional availability and OS

GCP

Note 1: GCP pricing is based on per hour consumption.

Note 2: Google Compute services vary between regional availability and OS

Exhibit A – Smartronix Managed Services Catalog

1.1. ACCOUNT SERVICES (REQUIRED)

1.1.1. ACCOUNT MANAGEMENT SERVICES (AMS)

The CAMS Account Management Service (AMS) is optimized to enforce and report CIS Benchmark Compliance and provide event trail aggregation and analysis. Security Benchmarks are defined and monitored in accordance with CAMS/CIS best-practices, which are made up of hundreds of industry-standard checks. Environments are audited to ensure security compliance, against relevant standards.

Scope:

- CSP Account Event Trails: AWS CloudTrail, Azure Monitor Logs, GCP StackDriver Metrics
- Object Storage Security: AWS S3, Azure Storage Accounts, GCP Cloud Storage Buckets
- AWS/Azure/GCP CIS Benchmark Compliance Implementation/Auditing/Reporting at the Account/Subscription/Project level

Standard Audited CSP Events:

- Privileged (root) Login
- Non-MFA Login
- Identity and Access Management changes to Policies, Groups, Users and Roles
- Notification of new Security Groups and changes to existing Security Groups
- Object Storage Policies/ACL changes
- Public access grant notifications for Object Storage
- Service Quota Limits

Automated Compliance Reporting:

- Reports on best practices and customer compliance with Center for Internet Security (CIS) benchmarks compared against the CSP IaaS environment and assets.
- Reports on existing Object Storage policies and potential risks (is the storage publicly accessible)

Account Management Triggers include:

*Triggers can be customized to customer workloads. Custom event types not identified below can be created/deployed and actioned directly to the customer as a professional services effort.

Root account logins	CSP Login authentication failures
Object storage policy changes	Security group changes
IAM policy changes	Network ACL changes
Logins without MFA	Change to cloud network gateway
CloudTrail configuration changes	Network route table changes

1.1.2. EVENT MANAGEMENT & INCIDENT RESPONSE

The Smartronix' Event Management and Incident Response (EM&IR) Service supports identification, classification, and filtering of Events, as well as structured response for mitigation and remediation of exception Incidents within customer environments.

Event management includes detection and notification via the CAMS Monitoring Solution (CMS) automation framework. Events are filtered via notification service topics and registered as Informational, Warning, or Exception.

Event Warnings initiate low priority Incident response workflows. Exception Events trigger high priority Incident response processes and procedures. The Smartronix' CloudAssured team employs structured processes for the identification, classification, escalation where necessary, and remediation of managed cloud infrastructure and supported operating system incidents.

1.1.3. SLA MANAGEMENT

Customer service requirements are monitored and tracked against documented Service Level Agreements (SLAs). The SLA Management Service reports service performance against standard Service Level targets identified below in Section 3. The reports are provided periodically and are designed to ensure service transparency by providing quality metrics throughout your experience. These metrics become the baseline for our ITSM Continuous Process Improvement.

1.1.4. LOG AGGREGATION SERVICE

Smartronix' Log Aggregation (LA) Service captures cloud service provider logs, guest OS logs for managed instances, and network logs. Alerts are generated for critical events and key performance indicators within the environment, which then automatically trigger an operational response.

Using the LA Service and Smartronix' change management process, the CloudAssured team monitors the IaaS environment for possible security incidents through event filters and alerts and performs change management of event filters implemented to ensure known critical events are identified and escalated. This service is filter-driven by a set of unwanted event types. These events include items such as cloud infrastructure configuration changes, instance termination, and excessive CPU utilization. These event filters are customized through-out the MSP term as patterns develop from lessons learned specific to the customer's applications.

Please note that log correlation, advanced search, and analysis is not part of this service – see Security Services – Enhanced Log Aggregation and Analysis. Technologies used in support of log aggregation include:

- CSP API Logs
- Virtual Network Flow Logs
- Object Storage Access Logs
- CSP Service Log Streams
- OS Logs (agent required for managed instances)

1.1.5. BOUNDARY MANAGEMENT

Smartronix' Boundary Management (BM) Service is a proactive monitoring and management service providing configuration management of cloud service provider components for networking, firewalls, virtual private networking (VPN), subnets, access control lists (ACLs), and virtual networks.

Our CloudAssured team will manage and monitor boundary protection and cloud environment network operations to ensure a secure and highly-available environment for customer data and applications. The BM service identifies, mitigates, and implements network level changes in response to events or customer requests. Supported change requests include VPN tunnel configuration, firewall policy changes to ACLs, IP route configurations, public IP allocation for service advertising, deployment of load balancing capabilities, and deployment of new cloud IP subnets. Technologies used in support of boundary management include:

- Network Flow Logs
- CSP API Event Logs
- M&N for ACL and Security Group changes

1.1.6. INFRASTRUCTURE PROVISIONING

Smartronix Infrastructure Provisioning (IP) services ensure consistent and repeatable deployment of cloud infrastructure. Customers submit IP requests through the CloudAssured ITSM portal for any service that requires management. Smartronix receives the requests, confirms the requirements, provisions the resource, and instruments the resource to ensure any core or additionally procured managed service is configured appropriately for M&N, SLA, ER&IR, AMS, BU, PM, and LA services.

Core Infrastructure Provisioning covers:

- Compute
- Storage
- Boundary Configuration
- Identity and Access Management Credentials
- Load Balancers
- Workspace provisioning

1.2. CORE SERVICES (INSTANCE BASED)

Smartronix core services integrate with the established Event Management and Incident Response and ITSM Portal for Service Request Management.

1.2.1. MONITORING AND NOTIFICATION SERVICE

The Smartronix M&N Service leverages the CAMS Monitoring Solution (CMS) automation framework. The CMS leverages micro services to detect all assets that are tagged for management and enables a defined set of standardized alarms/alerts. Each alarm can be customized to a tagged instance definition, allowing customer environments to have different defined alarm triggers for specific workloads. The CMS framework leverages web hooks to pull in the alarms/alerts and to automate creation of ITSM tickets.

Triggers include:

**Triggers can be customized to customer workloads. Custom event types not identified below can be created/deployed and actioned directly to the customer as a professional services effort.*

High CPU Utilization*	Instance failed health check
Disk space utilization*	Excessive network utilization*
Excessive disk IOPs*	High memory usage*
Excessive disk write queue length*	

1.2.2. OPERATING SYSTEM PATCH MANAGEMENT

Smartronix' Operating System Patch Management (PM) Service monitors the availability of and proactively applies operating system patches and updates through the use of a patch management life-cycle. Smartronix' CloudAssured team performs monthly patching of guest operating systems based on the vendor release schedule. Maintenance and patching windows are coordinated with each customer to ensure operations are not impacted by system patching. The patching capability is a scripted process that will trigger the guest OS to download and apply the identified guest OS patches. The applied patches are tracked through the CloudAssured MSP system to track system configuration. Critical or security related patches are quickly escalated to the customer for approval to deploy during an out of cycle maintenance window.

Customers can opt-in (patch and update) or opt-out (do not patch, do not update) individual systems via the instance tag.

Supported Operating Systems include:

- Amazon Linux 2015.03+
- RedHat Enterprise Linux
- CentOS 6/7
- Ubuntu 12.04/14.04 LTS
- Windows 2008-2019

1.2.3. ANTI-MALWARE MANAGEMENT SERVICE

Smartronix' Anti-malware (AMS) Management Service protects your environment against malware (viruses, trojans, spyware/grayware) by ensuring that the CAMS provided antimalware is installed, up-to-date, active, and is running current malware signatures on managed OS instances. When malware is detected, we proactively ensure quarantine and automatically create an incident ticket for the remediation of the issue. Audits are performed to ensure individual server compliance with customer antimalware policies.

The service is provided through a consolidated management framework. Smartronix' CloudAssured MSP offering leverages distributed relays and customer policy-based isolation. The AMS functionality is currently provided by the TrendMicro Deep Security Suite (DSS). Smartronix deploys the Deep Security Agent (DSA) on the customer guest OS image. These instances are registered through the customer DSA relay and transmitted through encrypted IP-restricted transport to the CloudAssured Deep Security Manager (DSM). Through the DSM, policies are applied to customer agents to ensure signature updates

are applied as soon as available to enable up-to-date protection of customer systems. Customers can request custom agent exclusions through the CloudAssured ServiceNow portal.

The anti-malware service protects against many file-based threats, including the following: Viruses (file infectors), Trojans, Backdoors, Worms, Network, Rootkits, Spyware, Grayware, packers, and keyloggers.

BU Services includes scheduled point in time disk volume snapshots to backup iterations of the storage volume. The service can be customized to retain backups for a customer-specified duration. The duration of backup retention will have an impact on cloud storage costs. Through the ITSM process, the CloudAssured team can restore system volumes to a customer-specified point-in-time. Prior to restoration of the requested volumes, a new snapshot will be captured to ensure a rollback is available if the restore is unsuccessful. Backup and restore testing is performed annually to ensure backup consistency.

1.3. OPTIONAL MANAGED SERVICES

1.3.1. CSEM ADVISORY

The Smartronix Cloud Service Expense Management (CSEM) Advisory Service facilitates environmental cost optimization based on actual usage data aggregation and correlation. Recommendations are based on analysis of CSEM actuals; application of advanced tool sets to model future spend as a function of utilization and execution of “what-if” scenarios; familiarity with customer workloads and environments; and, extensive experience across customer cloud environments. The CSEM Advisory Service is included as an integrated component of the Cloud Resale and Consolidated Billing Service.

Examples of cost optimization opportunities include:

- Resource utilization (Throttling under-utilized instances; Parking off-period resources)
- Right-sizing instance type
- Selection of workload-appropriate pricing models
- Resource tagging
- Reclamation of orphaned resources
- Optimization of BYOL (Bring-your-own-license)
- Storage life-cycle management
- Cost Monitoring and Alerting

This service requires deployment of the Smartronix CSEM tool which requires read only access to the CSP billing data and optional read only access to performance data (for service utilization optimization.)

1.3.2. INFRASTRUCTURE ADVISORY

Smartronix' Infrastructure Advisory (IA) Services provides prescriptive guidance on cloud services optimization, including capacity management reviews, architectural reviews and best practices reviews, auto scaling tuning, and migration paths for on premise workloads. These reviews leverage our CloudAssured - Well Architected guidelines and ITSM process.

The CloudAssured - Well Architected Review is a detailed analysis of your infrastructure, a thorough review of security practices, application integration architectures, and sizing of resources. This review enables Smartronix' CloudAssured team to ensure customers are leveraging cloud services in line with CSP best practices while delivering cost effective and secure service delivery.

1.3.3. DISASTER RECOVERY

Smartronix' Disaster Recovery (DR) Service defines a DR architecture and processes to provide full planning, annual testing and execution of a managed disaster recovery solution encompassing applications, systems, and environments. Our CloudAssured team will work with you to ensure your Recovery Time Objective/Recovery Point Objective (RTO/RPO) are appropriate to your mission and to architect the solution to fulfill the requirements at the lowest cost.

1.3.4. ADVANCED APPLICATION MONITORING

Smartronix' Advanced Application Monitoring (AAM) Service provides deeper visibility into your entire environment. Using header tags, synthetic transactions, agent-based health tools, and state-of-the-art tools, processes, and best practices, the Smartronix CloudAssured team will configure advanced monitoring to discover and optimize a comprehensive suite of availability and performance metrics.

1.3.5. ENHANCED DATA ENCRYPTION

Smartronix' Enhanced Data Encryption (EDE) Service is a custom solution. Smartronix' CloudAssured team works with the customer to define a service architecture compliant with their regulatory or policy requirements, and then implements the architecture with encryption built-in. The CAMS team provides all support for encryption key management and rotation, encryption of volumes and data, and implementation and management of service encryption certificates.

Areas of applicable support include:

- Use of cloud or collocated hardware security modules
- Database, disk volume, object store, and/or application level encryption
- End-to-end security – data ingestion, data at rest, data in transit, data in use, and data extraction
- Certificate management for secure protocols (SSL, HTTPS, TLS, etc.)
- Key lifecycle management (creation, deployment, expiration, rotation, invalidation)

1.3.6. APPLICATION MANAGEMENT

Smartronix' Application Management (AM) Service delivers COTS and custom-built applications under the managed Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) model. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

1.3.7. DATABASE MANAGEMENT

Smartronix' Database Management (DBM) Service is a full-lifecycle capability available for industry-leading RDBMSs. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

1.3.8. WEB MANAGEMENT AND CDN

Smartronix' Web Management and CDN (WMC) Service provides monitoring, availability, maintenance, security and configuration management for web applications and frameworks, including the operations and management of third party CDN services. We provide proactive security monitoring of the site distribution, availability monitoring, maintenance, configuration management, patching and security of the environment and applications. External availability and performance monitoring is also available.

1.3.9. WORKSPACES MANAGEMENT

Smartronix' Workspaces Managed Services (WMS) brings server-class management and assurance to virtual desktop users. WMS includes operating system patch and update management, software packaging, and software lifecycle management (deployment, configuration management, updating, and deprovisioning). Workspaces Management Services Backups let you choose an RPO that's right for your organization and know that your virtual workstation data is protected. Antivirus and antimalware are included, and compliance is enforced. Integration with your existing directory service means organizational configurations, policies, and controls are applied to your Workspaces and managed by Smartronix WMS the same as they are for your servers.

1.3.10. SERVERLESS COMPLIANCE, LOGGING, AND REAL-TIME MONITORING (SCLRM)

The CAMS SCLRM is optimized to monitor CSP Serverless implementations and enforce and report CIS Benchmark Compliance. Security Benchmarks are defined and monitored in accordance with CAMS/CIS best-practices, which are made up of hundreds of industry-standard checks. All serverless environments are audited to ensure security compliance, against relevant standards.

Scope:

- Serverless Monitoring and Notification: AWS Lambda, GCP Cloud Functions, Azure Function Apps
- AWS/Azure/GCP CIS Benchmark Compliance Implementation/Auditing/Reporting at the Account/Subscription/Project level

Serverless Event Monitoring and Notification:

- Captures all (CSP) events, logs, audit information, and monitoring information provided by in-scope services.
- Alerts are defined for key events within the environment to trigger further analysis or incident response.
- Monitored Metrics include:
 - Number of invocations
 - Failed executions (permissions, timeouts, exceptions)
 - Concurrent executions
 - Execution throttling

1.3.11. CONTAINER SERVICE MONITORING (ECSM)

The CAMS ECSM is a monitoring capability designed specifically for AWS Elastic Container Services.

The CAMS Monitoring Service (CMS) has been extended to support monitoring of tagged ECS clusters. The following metrics are automatically enabled across the cluster and services:

ECS Supported Metrics (Dimension)

- Cluster
 - CPUUtilization
 - MemoryUtilization

- CPUReservation
- MemoryReservation
- GPUReservation
- Service
 - CPUUtilization
 - MemoryUtilization

These metrics tie into the Event Management and Incident Response service for effective identification, classification, and remediation of metrics that exceed allowable thresholds.

1.3.12. CONTAINER SERVICE PATCH MANAGEMENT (ECSP)

The CAMS ECSP is a custom patching capability designed specifically for AWS Elastic Container Services.

AWS recommends updating your ECS containers instance fleet with the latest AMI whenever possible. This solution is triggered via a Set Schedule (time based Patch Window) or the AWS Event that is triggered whenever a new AMI is provided by AWS.

Both Events cause a change to the launch configuration to use the newest AMI ID. The new AMI is automatically placed into service and the old AMI is drain stopped and removed from service. This process is repeated until all nodes are using the latest AMI. Upon successful completion of the Patching the service provides an SNS notification indicating success. If a failure event occurs the solution rolls back to the previous launch configuration and a SNS notification is provided for further remediation.

1.4. MANAGED SECURITY SERVICES

1.4.1. SECURITY INCIDENT RESPONSE

Smartronix' Security Incident Response (SIR) Service provides analysis, tracking, and corrective actions for issues impacting customer environments. Smartronix' CloudAssured team will support the incident response process through incident escalation, break/fix remediation of infrastructure and guest operating systems, support of in-scope disaster recovery, system restore, instance isolation, and event information reporting related to the cloud environment and guest operating systems. The CloudAssured IR capability can also be leveraged by customer application teams to help identify application-impacting problems related to the environment or guest operating systems.

1.4.2. ENHANCED LOG AGGREGATION AND ANALYSIS

Smartronix' Enhanced Log Aggregation and Analysis (ELAA) Service captures events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.

ELAA extends the core *Log Aggregation* service by integrating search capabilities, counters, and proactive log review analysis. The *Analysis* capability enables the correlation of events by generating a process chain. For example, a web site health check failure can be linked to a john.doe login and a john.doe action of stopping the web service. The standard Log Aggregation event filter service will only identify the user logged on, the user stopped a service, or the web health check failed, but the causality link between events would be a manual process. The search capability also enhances the ability of the customer's applications teams to quickly identify underlying system events linked to a service incident.

1.4.3. HOST INTRUSION DETECTION/PREVENTION

Smartronix' Managed Host IDS/IPS service provides 24 x 7 security event alerting, investigation and response to potential security incidents identified by our endpoint HIDS/HIPS capability. The CAMS HIDS/HIPS service leverages industry partner-maintained and updates signature sets. The CAMS security team ensures the most appropriate sets of signatures are applied to customer endpoints. With systems and security managed services engineers, we provide immediate on-call and after-hours assistance to extend the IT security capability of your team.

1.4.4. HOST FILE INTEGRITY MONITORING

Smartronix' Host File Integrity monitoring service can alert you when changes happen to key operating system and application files, as well as essential processes and ports. Integrity monitoring detects unauthorized changes that introduce operational as well as security risks by identifying system incompatibilities and potential indicators of compromise (IOCs). The service leverages our FIM capability to provide alerts and response to identified events 24x7. The identification of protected files can be customized to meet customer security concerns.

1.4.5. SMARTRONIX CYBERHUNTER

A common challenge for system administrators and security analysts is determining if an instance has malware present or has been compromised. This may be due to many reasons, such as a security event detection, concerns that a "coin miner" is impacting instance CPU load, a security misconfiguration that may have resulted in instance compromise, or leadership seeking assurances that the environment has not been compromised by a recent threat. Performed manually, live system triage is time consuming, requires specialty knowledge, and is prone to error. Common methods of triage look for indicators of compromise that always lag behind the threat and often miss the most concerning attacks.

CyberHunter is a Smartronix developed capability for performing non-service impacting live system triage and compromise assessment. Our innovative detection techniques were developed based on our years of defending high value environments from the most sophisticated threat actors. CyberHunter merges our unique memory analysis methods with our knowledge of other key points of system analysis with automation of the collection and triage of systems. Proprietary, multi-faceted analytic and triage methods are then leveraged to provide our seasoned analysts with rich, high quality information to enable an accurate and prompt threat identification. Together our tools and analysts provide our customers assurance that their environment is threat free of malicious code. And when things go wrong and an adversary gains access, the Smartronix CyberHunter capability provides the advanced skills to help push the threat out.

1.4.6. SYSTEMS VULNERABILITY SCANNING

Smartronix' Systems Vulnerability Scanning Service utilizes Tenable's Nessus Security Scanner and Nessus Security Manager. The scanning service enables the assessment of networks and connected IT systems against regulatory compliance standards and identifies any known system vulnerabilities, the solution offers automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery.

Note: The standard template supported by the vulnerability scanning service is from the Center for Internet Security (CIS) benchmarks. Additional standards and templates may be supported based on customer regulatory requirements.

1.4.7. SECURITY AND REGULATORY COMPLIANCE ADVISORY SERVICES

Smartronix' Security and Regulatory Compliance Advisory (SRCA) Service leverages Smartronix' security compliance experts to provide clients guidance in meeting regulatory requirements and recommend mitigation of threats that have potential to impact client-specific environments as they appear and evolve. The service will help document and update control documentation in support of maintaining customer regulatory compliance.

Examples of compliance activities include:

- Creation of System Security Plan documentation
- Support of internal compliance audits
- Tracking Plans of Action and Milestones (POAMs)
- Risk assessment and planning
- Monitoring and responding to industry regulatory changes

1. SERVICE LEVEL AGREEMENTS

1.1. SLA 1: SYSTEM AVAILABILITY

SLA 1: "System" Availability	
Description	This SLA applies to "system availability" of a service. A system is considered a series of components that make up the infrastructure service that hosts and provides the compute and storage capabilities consumed by the customer applications and services. System availability applies to the following products and services: - Virtual Compute Instances (AWS EC2 and Azure Virtual Machines deployed in the same availability set) - Block Storage (AWS EBS, Azure System/Data Disks) Smartronix SLA incorporates the AWS and Azure SLA terms defined below which are subject to change in accordance with the AWS and Azure Agreements. - AWS Compute SLA: https://aws.amazon.com/ec2/sla/ - Microsoft Azure Compute SLA: https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_6/
Measurement	Smartronix will measure system infrastructure availability by using tools that will access the cloud infrastructure compute availability at 5 minute intervals to analyze cloud IaaS regional compute availability.
Calculation	NUMERATOR Uptime (Seconds) ÷ DENOMINATOR= Total amount of time (seconds) for the monitoring period = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if the system is fully available for use 99.95% of the time.
Exceptions / Conditions	Instances scheduled to occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: Downtime approved by customer; and Downtime due to events outside Smartronix control and approved as such by customer. Examples of these type of exception events include: Force majeure events; and Outages determined to be caused by customer or customer contractor-developed application code provided by customer. Systems must be implemented in a functional high availability configuration.

1.2. SLA 2: BACKUP AND RESTORATION

SLA 2: Backup and Restoration	
Description	This SLA measures the percent of times that the platform is restored to last agreed and documented state and last transactional dataset after failure, data loss or user request for restoration.
Measurement	Initiation of restore for individual file or database requests within 8 hours of receipt of request or notification of failure Backup retention periods are defined by Client.
Calculation	NUMERATOR: Number of successful restore initiations within 8 hours or Number of full restoration within 48 hours ÷ DENOMINATOR: Number of Requests for Restores = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully restored 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

1.3. SLA 3: INCIDENT RESPONSE

SLA 3: Incident Response Time	
Description	This SLA measures Smartronix' response time, per the Exceptions/Conditions in this SLA, following issue identification.
Measurement	SLA attainment is validated by 100% inspection of reporting documentation.
Calculation	NUMERATOR: Number of incidents receiving response within time for given severity level ÷ DENOMINATOR: Total number of Incidents = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is successful if 95% of incidents receive a response within response time for given severity level, as measured on a monthly basis.
Exceptions / Conditions	Severity 1 - Critical - An entire service is down. All users affected. Within 1 hour of incident occurring 24x7x365. Severity 2 - High - Operation of the service is severely degraded, or major components of the services are not available. Significant user impact. Within 2 hours of incident occurring 24x7x365. Severity 3 - Medium - Some non-essential features of the service are impaired or subject to interruptions while most vital components of the service remain

SLA 3: Incident Response Time

	functional. Minimal user impact. Within 24 hours of incident occurring during business hours. (8am-8pm EST M-F). Severity 4 - Low - Errors that are minor and clearly have little to or no impact on the normal operation of the service. No or minimal user impact. Within 1 business day of incident occurring during business hours. (8am-8pm EST M-F). Exception: Impending events; notification will happen; incident response will be initiated before follow-up notification; as clients will be previously notified (SLA 5) of the likelihood of the event.
--	--

1.4. SLA 4: OPERATING SYSTEM PATCHING AND UPDATING**SLA 4 – Operating System Patching**

Description	This SLA measures Smartronix' ability to patch all operating systems protecting on a planned schedule. All critical patches will be applied in accordance to the client planned schedule that will be defined in the Concept of Operations document. All other patches will be executed upon a customer pre-approved schedule.
Measurement	All operating systems will be up to date with critical patches within 10 days of release and measured by scanning with vulnerability software.
Calculation	NUMERATOR: Total number of patched systems within 10 calendar days of critical patch release ÷ DENOMINATOR: Number of systems requiring patches = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is considered successful when 95% of critical patches are applied to the initial environment within 10 calendar days of release from vendor and subsequent patches are applied per the customer patch schedule. Patches must be approved by customer. This will be measured on a monthly basis.
Exceptions / Conditions	Ten (10) day SLA applies to the initial environment patched. Patching of subsequent environments follow customer patch schedule. Smartronix failure to execute patching of subsequent environments per customer patch schedule shall also be considered an SLA failure for purposes of the Calculation. Any patches not approved by customer or Smartronix' CCB are excluded from the SLA Calculation.

1.5. SLA 5: IMPENDING EVENT NOTIFICATION**SLA 5 – Impending Event Notifications**

Description	Smartronix will notify the customer of the possibility of an impending event or events that have occurred which might affect system operation. Examples include cloud service provider notifying Smartronix of service degradation, service unavailability, or service termination.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending event.
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

1.6. SLA 6: DATABASE MANAGEMENT SERVICE REQUEST

SLA 6 – Service Request – Database Management	
Description	Smartronix will initiate requested support on-demand functions for Database support made by the customer within one business day. Examples include request for database refresh from prod to Test or development, launching database instances, performing performance analysis.
Measurement	Smartronix will measure request response based on the time requested as documented in the ITSM reporting system and the request initiation being within 1 business day.
Calculation	NUMERATOR: Number of successful request initiations within 1 business day ÷ DENOMINATOR: Number of Requests = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully initiated responses 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

1.7. SLA 7: IMPENDING SECURITY THREAT NOTIFICATION

SLA 7: Impending Security Threat Notifications	
Description	Smartronix will notify the Client of the possibility of an impending Security Threat or events that have occurred which may impact system operation. Examples include global intelligence sources identifying new threats in the environment that may impact OS, Applications, or services used by Client.

SLA 7: Impending Security Threat Notifications	
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending threat
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

*SLA usage can vary dependent on services purchased.

AWS PUBLIC SECTOR ACCESS POLICY

(Last Updated April 2, 2018)

This AWS Public Sector Access Policy (“**Access Policy**”) is hereby made a part of the agreement (the “**Agreement**”) between [INSERT END CUSTOMER NAME] (“**Customer**”) and [INSERT SOLUTION PROVIDER NAME] (“**Solution Provider**”) regarding Customer’s use of and access to the AWS Services via the AWS accounts provided to Customer by Provider (“**Solution Provider Accounts**”). Section 7 contains definitions of capitalized terms.

1. Scope. This Access Policy is not an agreement with Amazon Web Services, Inc. (“**AWS**”). It sets out the rules, conditions, and restrictions that apply to Customer’s use of the AWS Services under Solution Provider Accounts where (1) Customer does not have an AWS Services Agreement with AWS; or (2) if Customer does have an AWS Services Agreement with AWS, Solution Provider has not designated it to AWS as Customer’s own account under the AWS Solution Provider Program.

2. Use of the Services.

2.1 Generally. Solution Provider gives Customer access to the AWS Services via Solution Provider Accounts, and Customer’s use of and access to the AWS Services is governed by the Agreement and this Access Policy. Contractual commitments by AWS to Solution Provider (for example, service level agreements) do not apply as between Customer and AWS. Customer must look solely to Solution Provider under this Agreement regarding any claims or damages relating to, or arising out of, the AWS Services. Solution Provider is not an agent of AWS and is not acting on behalf of AWS, and Customer is not a third party beneficiary of any agreement between Solution Provider and AWS.

2.2 Disclaimers; Limitations on AWS Liability. THE AWS SERVICES, AWS CONTENT, AND THIRD-PARTY CONTENT ARE PROVIDED “AS IS.” EXCEPT TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, NEITHER AWS, NOR SOLUTION PROVIDER ON BEHALF OF AWS, MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT. AWS DISCLAIMS ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (a) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (b) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (c) THAT THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (d) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST, ALTERED, OR DAMAGED. AWS WILL NOT BE LIABLE TO CUSTOMER FOR ANY DAMAGES OF ANY KIND (INCLUDING DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, DAMAGES FOR LOST PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA, THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY CUSTOMER IN CONNECTION WITH CUSTOMER’S USE OF THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT) ARISING IN CONNECTION WITH, OR RELATED TO, CUSTOMER’S INABILITY TO USE THE AWS SERVICES, INCLUDING AS A RESULT OF ANY TERMINATION OR SUSPENSION OF SOLUTION PROVIDER ACCOUNTS UNDER ANY AGREEMENT BETWEEN AWS AND SOLUTION PROVIDER, DISCONTINUATION OR DOWNTIME OF AWS SERVICES, OR ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ACCOUNT CONTENT.

2.3 Account Keys. Solution Provider may provide Customer with AWS account keys which will allow Customer to directly access the AWS Services via Solution Provider Accounts. AWS is not responsible to Customer for any activities that occur under these account keys, regardless of whether the activities are undertaken by Customer, Solution Provider, or a third party (including Customer employees, contractors or agents) and AWS is not responsible to Customer for unauthorized access to Solution Provider Accounts.

2.4 Third-Party Content. Through the use of the AWS Services or the AWS Site, Customer may have access to Third-Party Content, which is made available directly to Customer by other entities or individuals under separate terms and conditions, including separate fees and charges. Customer’s use of any Third-Party Content is at its sole risk.

2.5 AWS Services Policies. All access to and use of AWS Services is subject to the AWS Services Policies. (Notwithstanding anything in the Acceptable Use Policy and AWS Service Terms, these two AWS Services Policies are not separate agreements between Customer and AWS.)

2.6 Customer Responsibilities. Unless otherwise agreed by Solution Provider, Customer is solely

responsible for the development, content, operation, maintenance, and use of Account Content in Solution Provider Accounts, including (a) the technical operation of AWS Services in connection with Account Content; (b) compliance of Account Content with the AWS Services Policies and applicable law; (c) any action Customer permits, assists, or facilitates any other person or entity to take under Solution Provider Accounts; and (d) use of AWS Services or Account Content by End Users under Solution Provider Accounts (and ensuring that End Users comply with Customer obligations under this Access Policy). If Customer becomes aware of any violation of its obligations under this Access Policy caused by itself or an End User, Customer will immediately terminate such End User's access to Account Content and the AWS Services by such End User. Unless otherwise agreed by Solution Provider, Customer is solely responsible for properly configuring and using the AWS Services and otherwise taking appropriate action to secure, protect, and backup Solution Provider Accounts and Account Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Account Content from unauthorized access and routinely archiving Account Content.

3. AWS Services Interruption. AWS may suspend the Solution Provider Accounts used by Customer to access the AWS Services immediately if AWS determines Customer's or an End User's use of the AWS Services (i) violates the AWS Services Policies; (ii) poses a security risk to the AWS Services or any other AWS customer, (iii) may harm AWS systems or the systems or Content of any other AWS customer; or (iv) may subject AWS to liability as a result of any of the foregoing. We will provide notice of any suspension to Solution Provider, who is solely responsible for providing any notices to Customer under the Agreement. Nothing in this Section 3 will operate to limit Customer's rights or remedies otherwise available to Customer against Solution Provider under the Agreement or applicable law.

4. Transition of Solution Provider Accounts. Except as otherwise provided by law or the Agreement, a transition of Solution Provider Accounts from Solution Provider to a third party (or directly to AWS) requires advance written consent by Solution Provider (which Solution Provider must also obtain from AWS). Customer agrees to cooperate with Solution Provider in transitioning Solution Provider Accounts, and to provide all appropriate information and take all appropriate action necessary to facilitate such transition. In any case, absent prior authorization by AWS, Customer may not transfer Solution Provider Accounts to other providers that are not authorized to resell AWS Services.

5. Proprietary Rights

5.1 Generally. AWS or its licensors own all right, title, and interest in and to the AWS Services, and all related technology and intellectual property rights. Customer (a) has the right to access and use the AWS Services under Solution Provider Accounts solely in accordance with this Access Policy and the Agreement, and (b) may copy and use the AWS Content provided by Solution Provider (or, as applicable, by AWS) solely in connection with Customer's permitted use of the AWS Services. Except as provided in this Section 5, Customer obtains no rights under this Access Policy from AWS, its affiliates, or Solution Provider to the AWS Services, the AWS Content, or Third-Party Content, including any related intellectual property rights. Some AWS Content and Third-Party Content may be provided to Customer under a separate license, such as the Apache License, Version 2.0, or other open source license. By using those materials, Customer is subject to such additional terms. Customer is solely responsible for securing any necessary approvals for the download and use of such materials.

5.2 Restrictions. Neither Customer nor any End User will use the AWS Services or AWS Content in any manner or for any purpose other than as expressly permitted by this Access Policy and the Agreement. Neither Customer nor any End User will, or will attempt to (a) modify, distribute, alter, tamper with, repair, or otherwise create derivative works of any AWS Content or Content included in the AWS Services (except to the extent Content included in the AWS Services is provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the AWS Services or apply any other process or procedure to derive the source code of any software included in the AWS Services (except to the extent applicable law doesn't allow this restriction), or (c) access or use the AWS Services in a way intended to avoid incurring fees or exceeding usage limits or quotas.

5.3 Suggestions. If Customer provides any Suggestions to AWS or its affiliates, AWS and its affiliates will be entitled to use the Suggestions without restriction. Customer hereby irrevocably assigns to AWS all right, title, and interest in and to the Suggestions and agrees to provide Customer and AWS any assistance required to document, perfect, and maintain AWS's rights in the Suggestions.

5.4 U.S. Government Rights. In accordance with Federal Acquisition Regulation (FAR) Sections 12.211 and 12.212, and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 227.7202-1 and 227.7202-3, the AWS Services are provided (as applicable) as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the AWS Services. If Customer is using the AWS Services on

behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Customer will immediately discontinue its use of the AWS Services (including any AWS Content).

6. Representations and Warranties. Customer represents and warrants to Solution Provider that (a) Customer's and its End Users' use of the AWS Services (including any use by its employees, personnel, and (except for Solution Provider) contractors) will not violate this Access Policy, including the AWS Services Policies; (b) Customer or its licensors own all right, title, and interest in and to Account Content; (c) Account Content (including the use, development, design, production, advertising, or marketing of Account Content) or the combination of Account Content with other applications, Content, or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) Customer's use of the AWS Services will not cause harm to any End User.

7. Definitions.

"Account Content" means Content that Customer or any End User (a) runs on the AWS Services, (b) causes to interface with the AWS Services, or (c) uploads to the AWS Services or otherwise transfer, process, use or store in connection with the AWS Services.

"AWS Content" means Content AWS makes available (either directly or indirectly) in connection with the AWS Services or on the AWS Site to allow or facilitate access to and use of the AWS Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Content does not include the AWS Services.

"AWS Services" means, collectively or individually (as applicable), the web services made commercially available by us to Solution Provider for use under this Access Policy, including (as applicable) those web services described in the AWS Service Terms.

"AWS Services Agreement" means the AWS Customer Agreement at <http://aws.amazon.com/agreement>, or other written agreement by and between AWS and Customer (if any) governing Customer's access to and use of the AWS Services.

"AWS Services Policies" means the following provisions (uses of the pronoun "you" shall refer to Customer):

- *AWS Acceptable Use Policy*, located at <http://aws.amazon.com/aup> (as it may be updated by AWS from time to time), which describes prohibited uses of the AWS Services and the AWS Site;
- *AWS Service Terms*, located at <http://aws.amazon.com/serviceterms> (as they may be updated by AWS from time to time), which include the rights and restrictions for particular AWS Services;
- *AWS Site Terms*, located at <http://aws.amazon.com/terms/> (as they may be updated by AWS from time to time), which govern the use of the AWS Site; and
- All restrictions described in the AWS Content and on the AWS Site.

"AWS Site" means <http://aws.amazon.com> and any successor or related site designated by AWS.

"Content" means software (including machine images), data, text, audio, video or images.

"Documentation" means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals, instructions and specifications for the Services currently located at <http://aws.amazon.com/documentation>, as such documentation may be updated by us from time to time.

"End Customer Account" means an AWS account designated as such under the AWS Solution Provider Program, through which AWS Services are provided by Solution Provider to Customer, and in connection with which AWS and Customer have an AWS Services Agreement.

"End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Account Content; or (b) otherwise accesses or uses the AWS Services under Solution Provider Accounts. The term "End User" does not include individuals or entities when they are accessing or using the AWS Services or any Content under their own AWS account, rather than Solution Provider Accounts.

"Solution Provider Accounts" means Solution Provider's AWS accounts through which AWS Services are provided by Solution Provider to Customer.

“Suggestions” means all suggested improvements to the AWS Services or AWS Content that Customer provides to AWS or its affiliates.

“Third-Party Content” means Content made available to Customer by any third party on the AWS Site or in conjunction with the AWS Services.

Microsoft Customer Agreement

This Microsoft Customer Agreement (the “Agreement”) is between Customer and Microsoft and consists of these General Terms, the applicable Use Rights and SLAs, and any additional terms Microsoft presents when an order is placed. This Agreement takes effect when the Customer accepts these General Terms. The individual who accepts these General Terms represents that he or she is authorized to enter into this Agreement on behalf of the Customer.

General Terms

These General Terms apply to all of Customer’s orders under this Agreement. Capitalized terms have the meanings given under “Definitions.”

License to use Microsoft Products

- a. **License grant.** Products are licensed and not sold. Upon Microsoft’s acceptance of each order and subject to Customer’s compliance with this Agreement, Microsoft grants Customer a nonexclusive and limited license to use the Products ordered as provided in the applicable Use Rights and this Agreement. These licenses are solely for Customer’s own use and business purposes and are nontransferable except as expressly permitted under this Agreement or applicable law.
- b. **Duration of licenses.** Licenses granted on a subscription basis expire at the end of the applicable subscription period unless renewed. Licenses granted for metered Products billed periodically based on usage continue as long as Customer continues to pay for its usage of the Product. All other licenses become perpetual upon payment in full.
- c. **Applicable Use Rights.** For perpetual licenses, the Use Rights in effect when Customer orders a Product will apply. For subscriptions, the Use Rights in effect at the start of each subscription period will apply. Customers with subscriptions for Software may use new versions released during the subscription period subject to the Use Rights in effect when those versions are released. For metered Products billed periodically based on usage, the Use Rights in effect at the start of each billing period will apply during that period. Microsoft may update the Use Rights periodically, but material adverse changes for a particular version will not apply during the applicable license, subscription, or billing period.
- d. **End Users.** Customer will control access to and use of the Products by End Users and is responsible for any use of the Products that does not comply with this Agreement.
- e. **Affiliates.** Customer may order Products for use by its Affiliates. If it does, the licenses granted to Customer under this Agreement will apply to such Affiliates, but Customer will have the sole right to enforce this Agreement against Microsoft. Customer will remain responsible for all obligations under this Agreement and for its Affiliates’ compliance with this Agreement.
- f. **Reservation of Rights.** Microsoft reserves all rights not expressly granted in this Agreement. Products are protected by copyright and other intellectual property laws and international treaties. No rights will be granted or implied by waiver or estoppel. Rights to access or use a

Product on a device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.

- g. Restrictions. Except as expressly permitted in this Agreement or Product documentation, Customer must not (and is not licensed to):
- (1) reverse engineer, decompile, or disassemble any Product, or attempt to do so;
 - (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms;
 - (3) work around any technical limitations in a Product or restrictions in Product documentation;
 - (4) separate and run parts of a Product on more than one device;
 - (5) upgrade or downgrade parts of a Product at different times;
 - (6) transfer parts of a Product separately; or
 - (7) distribute, sublicense, rent, lease, or lend any Products, in whole or in part, or use them to offer hosting services to a third party.
- h. License transfers. Customer may only transfer fully-paid, perpetual licenses to (1) an Affiliate or (2) a third party solely in connection with the transfer of hardware to which, or employees to whom, the licenses have been assigned as part of (a) a divestiture of all or part of an Affiliate or (b) a merger involving Customer or an Affiliate. Upon such transfer, Customer must uninstall and discontinue using the licensed Product and render any copies unusable. Customer must notify Microsoft of a License transfer and provide the transferee a copy of these General Terms, the applicable Use Rights and any other documents necessary to show the scope, purpose and limitations of the licenses transferred. Attempted license transfers that do not comply with this section are void.
- i. Customer Eligibility. Customer agrees that if it is purchasing academic, government or nonprofit offers, Customer meets the respective eligibility requirements (<https://aka.ms/eligibilitydefinition>). Microsoft reserves the right to verify eligibility and suspend product use if requirements are not met.

Non-Microsoft Products.

Non-Microsoft Products are provided under separate terms by the Publishers of such products. Customer will have an opportunity to review those terms prior to placing an order for a Non-Microsoft Product through a Microsoft online store or Online Service. Microsoft is not a party to the terms between Customer and the Publisher. Microsoft may provide Customer's contact information and transaction details to the Publisher. Microsoft makes no warranties and assumes no responsibility or liability whatsoever for Non-Microsoft Products. Customer is solely responsible for its use of any Non-Microsoft Product.

Verifying compliance.

Customer must keep records relating to Products it and its Affiliates use or distribute. At Microsoft's expense, Microsoft may verify Customer's and its Affiliates' compliance with this Agreement at any time upon 30 days' notice. To do so, Microsoft may engage an independent auditor (under nondisclosure obligations) or ask Customer to complete a self-audit process. Customer must promptly provide any information and documents that Microsoft or the auditor reasonably requests related to the verification and access to systems running the Products. If verification or self-audit reveals any unlicensed use, Customer must, within 30 days, order sufficient licenses to cover the period of its unlicensed use. Without limiting Microsoft's other remedies, if unlicensed use is 5% or more of Customer's total use of all Products, Customer must reimburse Microsoft for its costs incurred in verification and acquire sufficient licenses to cover its unlicensed use at 125% of the then-current Customer price or the maximum allowed under applicable law, if less. All information and reports related to the verification process will be Confidential Information and used solely to verify compliance.

Privacy.

- a. **Personal Data.** Customer consents to the processing of Personal Data by Microsoft and its Affiliates, and their respective agents and subcontractors, as provided in this Agreement. Before providing Personal Data to Microsoft, Customer will obtain all required consents from third parties (including Customer's contacts, Partners, distributors, administrators, and employees) under applicable privacy and data protection laws.
- b. **Location of Personal Data.** To the extent permitted by applicable law, Personal Data collected under this Agreement may be transferred, stored and processed in the United States or any other country in which Microsoft or its Affiliates, or their respective agents and subcontractors, maintain facilities. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland.

Confidentiality.

- a. **Confidential Information.** "Confidential Information" is non-public information that is designated "confidential" or that a reasonable person should understand is confidential, including, but not limited to, Customer Data, the terms of this Agreement, and Customer's account authentication credentials. Confidential Information does not include information that (1) becomes publicly available without a breach of a confidentiality obligation; (2) the receiving party received lawfully from another source without a confidentiality obligation; (3) is independently developed; or (4) is a comment or suggestion volunteered about the other party's business, products or services.
- b. **Protection of Confidential Information.** Each party will take reasonable steps to protect the other's Confidential Information and will use the other party's Confidential Information only for purposes of the parties' business relationship. Neither party will disclose Confidential Information to third parties, except to its Representatives, and then only on a need-to-know basis under nondisclosure obligations at least as protective as this Agreement. Each

party remains responsible for the use of Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party. The Online Services Terms may provide additional terms regarding the disclosure and use of Customer Data.

- c. Disclosure required by law. A party may disclose the other's Confidential Information if required by law, but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order.
- d. Residual information. Neither party is required to restrict work assignments of its Representatives who have had access to Confidential Information. Each party agrees that the use of information retained in Representatives' unaided memories in the development or deployment of the parties' respective products or services does not create liability under this Agreement or trade secret law, and each party agrees to limit what it discloses to the other accordingly.
- e. Duration of Confidentiality obligation. These obligations apply (1) for Customer Data, until it is deleted from the Online Services; and (2) for all other Confidential Information, for a period of five years after a party receives the Confidential Information.

Product warranties.

a. Limited warranties and remedies.

- (1) Online Services. Microsoft warrants that each Online Service will perform in accordance with the applicable SLA during Customer's use. Customer's remedies for breach of this warranty are described in the SLA.
- (2) Software. Microsoft warrants that the Software version that is current at the time will perform substantially as described in the applicable Product documentation for one year from the date Customer acquires a license for that version. If it does not, and Customer notifies Microsoft within the warranty term, Microsoft will, at its option, (a) return the price Customer paid for the Software license or (b) repair or replace the Software.

The remedies above are Customer's sole remedies for breach of the warranties in this section. Customer waives any warranty claims not made during the warranty period.

- b. Exclusions. The warranties in this Agreement do not apply to problems caused by accident, abuse, or use inconsistent with this Agreement, including failure to meet minimum system requirements. These warranties do not apply to free, trial, preview, or prerelease products, or to components of Products that Customer is permitted to redistribute.
- c. Disclaimer. Except for the limited warranties above and subject to applicable law, Microsoft provides no other warranties or conditions for Products and disclaims any other express, implied or statutory warranties for Products, including warranties of quality, title, non-infringement, merchantability, and fitness for a particular purpose.

Defense of third-party claims.

The parties will defend each other against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if the defending party is promptly notified in writing of the claim and has the right to control the defense and any settlement of it. The party being defended must provide the defending party with all requested assistance, information, and authority. The defending party will reimburse the other party for reasonable out-of-pocket expenses it incurs in providing assistance. This section describes the parties' sole remedies and entire liability for such claims.

- a. By Microsoft. Microsoft will defend Customer against any third-party claim to the extent it alleges that a Product made available by Microsoft for a fee and used within the scope of the license granted under this Agreement (unmodified from the form provided by Microsoft and not combined with anything else), misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party. If Microsoft is unable to resolve a claim of misappropriation or infringement, it may, at its option, either (1) modify or replace the Product with a functional equivalent or (2) terminate Customer's license and refund any license fees (less depreciation for perpetual licenses), including amounts paid in advance for unused consumption for any usage period after the termination date. Microsoft will not be liable for any claims or damages due to Customer's continued use of a Product after being notified to stop due to a third-party claim.
- b. By Customer. To the extent permitted by applicable law, Customer will defend Microsoft and its Affiliates against any third-party claim to the extent it alleges that: (1) any Customer Data or Non-Microsoft Product hosted in an Online Service by Microsoft on Customer's behalf misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party; or (2) Customer's use of any Product, alone or in combination with anything else, violates the law or harms a third party.

Limitation of liability.

For each Product, each party's maximum, aggregate liability to the other under this Agreement is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the Products during the term of the applicable licenses, subject to the following:

- a. Subscriptions. For Products ordered on a subscription basis, Microsoft's maximum liability to Customer for any incident giving rise to a claim will not exceed the amount Customer paid for the Product during the 12 months before the incident.
- b. Free Products and distributable code. For Products provided free of charge and code that Customer is authorized to redistribute to third parties without separate payment to Microsoft, Microsoft's liability is limited to direct damages finally awarded up to US\$5,000.
- c. Exclusions. In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, or loss of use, loss of profits, or interruption of business, however caused or on any theory of liability.
- d. Exceptions. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations (except for liability related to Customer Data, which will remain

subject to the limitations and exclusions above); (2) defense obligations; or (3) violation of the other party's intellectual property rights.

Partners.

- a. **Selecting a Partner.** Customer may authorize a Partner to place orders on Customer's behalf and manage Customer's purchases by associating the Partner with its account. If the Partner's distribution right is terminated, Customer must select an authorized replacement Partner or purchase directly from Microsoft. Partners and other third parties are not agents of Microsoft and are not authorized to enter into any agreement with Customer on behalf of Microsoft.
- b. **Partner Administrator privileges and access to Customer Data.** If Customer purchases Online Services from a Partner or chooses to provide a Partner with administrator privileges, that Partner will be the primary administrator of the Online Services and will have administrative privileges and access to Customer Data and Administrator Data. Customer consents to Microsoft and its Affiliates providing the Partner with Customer Data and Administrator Data for purposes of provisioning, administering and supporting (as applicable) the Online Services. Partner may process such data according to the terms of Partner's agreement with Customer, and its privacy commitments may differ from Microsoft's. Customer appoints Partner as its agent for purposes of providing and receiving notices and other communications to and from Microsoft. Customer may terminate the Partner's administrative privileges at any time.
- c. **Support and Professional Services.** Customer's Partner will provide details on support services available for Products purchased under this agreement. Support services may be performed by Partner or its designee, which in some cases may be Microsoft. If Customer purchases Professional Services under this agreement, the performance of those Professional Services will be subject to the terms and conditions in the Use Rights.

Pricing and payment.

If Customer orders from a Partner, the Partner will set Customer's pricing and payment terms for that order, and Customer will pay the amount due to the Partner. Pricing and payment terms related to orders placed by Customer directly with Microsoft are set by Microsoft, and Customer will pay the amount due as described in this section.

- a. **Payment method.** Customer must provide a payment method or, if eligible, choose to be invoiced for purchases made on its account. By providing Microsoft with a payment method, Customer (1) consents to Microsoft's use of account information regarding the selected payment method provided by the issuing bank or applicable payment network; (2) represents that it is authorized to use that payment method and that any payment information it provides is true and accurate; (3) represents that the payment method was established and is used primarily for commercial purposes and not for personal, family or household use; and (4) authorizes Microsoft to charge Customer using that payment method for orders under this Agreement.

- b. **Invoices.** Microsoft may invoice eligible Customers. Customer's ability to elect payment by invoice is subject to Microsoft's approval of Customer's financial condition. Customer authorizes Microsoft to obtain information about Customer's financial condition, which may include credit reports, to assess Customer's eligibility for invoicing. Unless the Customer's financial statements are publicly available, Customer may be required to provide their balance sheet, profit and loss and cash flow statements to Microsoft. Customer may be required to provide security in a form acceptable to Microsoft to be eligible for invoicing. Microsoft may withdraw Customer's eligibility at any time and for any reason. Customer must promptly notify Microsoft of any changes in its company name or location and of any significant changes in the ownership, structure, or operational activities of the organization.
- c. **Invoice Payment terms.** Each invoice will identify the amounts payable by Customer to Microsoft for the period corresponding to the invoice. Customer will pay all amounts due within thirty (30) calendar days following the invoice date.
- d. **Late Payment.** Microsoft may, at its option, assess a late fee on any payments to Microsoft that are more than fifteen (15) calendar days past due at a rate of two percent (2%) of the total amount payable, calculated and payable monthly, or the highest amount allowed by law, if less.
- e. **Cancellation fee.** If a subscription permits early termination and Customer cancels the subscription before the end of the subscription or billing period, Customer may be charged a cancellation fee.
- f. **Recurring Payments.** For subscriptions that renew automatically, Customer authorizes Microsoft to charge Customer's payment method periodically for each subscription or billing period until the subscription is terminated. By authorizing recurring payments, Customer authorizes Microsoft to process such payments as either electronic debits or fund transfers, or as electronic drafts from the designated bank account (in the case of Automated Clearing House or similar debits), as charges to the designated card account (in the case of credit card or similar payments) (collectively, "Electronic Payments"). If any payment is returned unpaid or if any credit card or similar transaction is rejected or denied, Microsoft or its service providers reserve the right to collect any applicable return item, rejection or insufficient funds fee to the maximum extent permitted by applicable law and to process any such fees as an Electronic Payment or to invoice Customer for the amount due.
- g. **Taxes.** Microsoft prices exclude applicable taxes unless identified as tax inclusive. If any amounts are to be paid to Microsoft, Customer shall also pay any applicable value added, goods and services, sales, gross receipts, or other transaction taxes, fees, charges, or surcharges, or any regulatory cost recovery surcharges or similar amounts that are owed under this Agreement and that Microsoft is permitted to collect from Customer. Customer shall be responsible for any applicable stamp taxes and for all other taxes that it is legally obligated to pay including any taxes that arise on the distribution or provision of Products by Customer to its Affiliates. Microsoft shall be responsible for all taxes based upon its net income, gross receipts taxes imposed in lieu of taxes on income or profits, and taxes on its property ownership.

If any taxes are required to be withheld on payments invoiced by Microsoft, Customer may deduct such taxes from the amount owed and pay them to the appropriate taxing authority, but only if Customer promptly provides Microsoft an official receipt for those withholdings and other documents reasonably requested to allow Microsoft to claim a foreign tax credit or refund. Customer will ensure that any taxes withheld are minimized to the extent possible under applicable law.

Term and termination.

- a. Term. This Agreement is effective until terminated by a party, as described below.
- b. Termination without cause. Either party may terminate this Agreement without cause on 60 days' notice. Termination without cause will not affect Customer's perpetual licenses, and licenses granted on a subscription basis will continue for the duration of the subscription period(s), subject to the terms of this Agreement.
- c. Termination for cause. Without limiting other remedies it may have, either party may terminate this Agreement on 30 days' notice for material breach if the other party fails to cure the breach within the 30-day notice period. Upon such termination, the following will apply:
 - (1) All licenses granted under this Agreement will terminate immediately except for fully-paid, perpetual licenses.
 - (2) All amounts due under any unpaid invoices shall become due and payable immediately. For metered Products billed periodically based on usage, Customer must immediately pay for unpaid usage as of the termination date.
 - (3) If Microsoft is in breach, Customer will receive a credit for any subscription fees, including amounts paid in advance for unused consumption for any usage period after the termination date.
- d. Suspension. Microsoft may suspend use of an Online Service without terminating this Agreement during any period of material breach. Microsoft will give Customer notice before suspending an Online Service when reasonable.
- e. Termination for regulatory reasons. Microsoft may modify, discontinue, or terminate a Product in any country or jurisdiction where there is any current or future government regulation, obligation, or other requirement, that (1) is not generally applicable to businesses operating there; (2) presents a hardship for Microsoft to continue offering the Product without modification; or (3) causes Microsoft to believe these terms or the Product may conflict with any such regulation, obligation, or requirement. If Microsoft terminates a subscription for regulatory reasons, Customer will receive, as its sole remedy, a credit for any subscription fees, including amounts paid in advance for unused consumption for any usage period after the termination date.

Miscellaneous.

- a. Independent contractors. The parties are independent contractors. Customer and Microsoft each may develop products independently without using the other's Confidential Information.

- b. Agreement not exclusive. Customer is free to enter into agreements to license, use, and promote the products and services of others.
- c. Amendments. Microsoft may modify this Agreement from time to time. Changes to the Use Rights will apply as provided in this Agreement. Changes to other terms will not apply until Customer accepts them. Microsoft may require Customer to accept revised or additional terms before processing a new order. Any additional or conflicting terms and conditions contained in a purchase order or otherwise presented by Customer are expressly rejected and will not apply.
- d. Assignment. Either party may assign this Agreement to an Affiliate, but it must notify the other party in writing of the assignment. Customer consents to the assignment to an Affiliate or third party, without prior notice, of any rights Microsoft may have under this Agreement to receive payment and enforce Customer's payment obligations, and all assignees may further assign such rights without further consent. Any other proposed assignment of this Agreement must be approved by the non-assigning party in writing. Assignment will not relieve the assigning party of its obligations under the assigned Agreement. Any attempted assignment without required approval will be void.
- e. U.S. export. Products are subject to U.S. export jurisdiction. Customer must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end use and destination restrictions by U.S. and other governments related to Microsoft products, services, and technologies.
- f. Severability. If any part of this Agreement is held to be unenforceable, the rest of the Agreement will remain in full force and effect.
- g. Waiver. Failure to enforce any provision of this Agreement will not constitute a waiver. Any waiver must be in writing and signed by the waiving party.
- h. No third-party beneficiaries. This Agreement does not create any third-party beneficiary rights except as expressly provided by its terms.
- i. Survival. All provisions survive termination of this Agreement except those requiring performance only during the term of the Agreement.
- j. Notices. Notices must be in writing and will be treated as delivered on the date received at the address, date shown on the return receipt, email transmission date, or date on the courier or fax confirmation of delivery. Notices to Microsoft must be sent to the following address:

Microsoft Corporation
Dept. 551, Volume Licensing
6100 Neil Road, Suite 210
Reno, Nevada 89511-1137
USA

Notices to Customer will be sent to the individual at the address Customer identifies on its account as its contact for notices. Microsoft may send notices and other information to Customer by email or other electronic form.

- k. Applicable law. This Agreement will be governed by and construed in accordance with the laws of the State of Washington and federal laws of the United States. The 1980 United Nations Convention on Contracts for the International Sale of Goods and its related instruments will not apply to this Agreement.
- l. Dispute resolution. When bringing any action arising under this Agreement, the parties agree to the following exclusive venues:
 - (1) If Microsoft brings the action, the venue will be where Customer has its headquarters.
 - (2) If Customer brings the action against Microsoft or any Microsoft Affiliate located outside of Europe, the venue will be the state or federal courts in King County, State of Washington, USA.
 - (3) If Customer brings the action against Microsoft or any Microsoft Affiliate located in Europe, and not also against Microsoft or a Microsoft Affiliate located outside of Europe, the venue will be the Republic of Ireland.

The parties consent to personal jurisdiction in the agreed venue. This choice of venue does not prevent either party from seeking injunctive relief in any jurisdiction with respect to a violation of intellectual property rights or confidentiality obligations.

- m. Order of precedence. These General Terms will take precedence over any conflicting terms in other documents that are part of this Agreement that are not expressly resolved in those documents, except that conflicting terms in the Use Rights take precedence over these General Terms as to the applicable Products. Terms in the Online Services Terms take precedence over conflicting terms in the Product Terms. Terms in an amendment control over the amended document and any prior amendments concerning the same subject matter.
- n. Microsoft Affiliates and contractors. Microsoft may perform its obligations under this Agreement through its Affiliates and use contractors to provide certain services. Microsoft remains responsible for their performance.
- o. Government procurement rules. By accepting this agreement, Customer represents and warrants that (i) it has complied and will comply with all applicable government procurement laws and regulations; (ii) it is authorized to enter into this Agreement; and (iii) this Agreement satisfies all applicable procurement requirements.

Definitions.

“Administrator Data” means the information provided to Microsoft or its Affiliates during sign-up, purchase, or administration of Products.

“Affiliate” means any legal entity that controls, is controlled by, or is under common control with a party. “Control” means ownership of more than a 50% interest of voting securities in an entity or the power to direct the management and policies of an entity.

“Confidential Information” is defined in the “Confidentiality” section.

“Customer” means the entity identified as such on the account associated with this Agreement.

“Customer Data” means all data, including all text, sound, software, image or video files that are provided to Microsoft or its Affiliates by, or on behalf of, Customer and its Affiliates through use of Online Services.

“End User” means any person Customer permits to use a Product or access Customer Data. “Licensing Site” means <http://www.microsoft.com/licensing/contracts> or a successor site. “Microsoft” means Microsoft Corporation.

“Non-Microsoft Product” means any third-party-branded software, data, service, website or product, unless incorporated by Microsoft in a Product.

“Online Services” means Microsoft-hosted services to which Customer subscribes under this Agreement. It does not include software and services provided under separate license terms.

“Online Services Terms” means the additional terms that apply to Customer’s use of Online Services published on the Licensing Site and updated from time to time.

“Partner” means a company Microsoft has authorized to distribute Products to Customer. “Personal Data” means any information relating to an identified or identifiable natural person. “Product” means all Software and Online Services identified in the Product Terms that Microsoft offers under this Agreement, including previews, prerelease versions, updates, patches and bug fixes from Microsoft. Product availability may vary by region. “Product” does not include Non-Microsoft Products.

“Product Terms” means the document that provides information about Products available under this Agreement. The Product Terms document is published on the Licensing Site and is updated from time to time.

“Publisher” means a provider of a Non-Microsoft Product.

“Representatives” means a party’s employees, Affiliates, contractors, advisors and consultants.

“SLA” means Service Level Agreement, which specifies the minimum service level for the Online Services and is published on the Licensing Site.

“Software” means licensed copies of Microsoft software identified in the Product Terms. Software does not include Online Services, but Software may be part of an Online Service.

“use” means to copy, download, install, run, access, display, use or otherwise interact with.

“Use Rights” means the license terms and terms of service for each Product published on the Licensing Site and updated from time to time. The Use Rights supersede the terms of any end user license agreement that accompanies a Product. License terms for all Products are published in the Product Terms. Terms of service for Online Services are published in the Online Services Terms.

Microsoft Customer Agreement

US Government Community Cloud

This Microsoft Customer Agreement is incorporated into the Customer Agreement and entered into between the customer who is a Community member ("Customer") and the person or entity who has entered into a prime contract with the Customer ("Contractor") as an addendum and governs Customer's use of the Microsoft Products. It consists of the terms and conditions below, Use Rights, SLA, and all documents referenced within those documents (together, the "agreement"). It is effective on the date that the Contractor provisions the Customer's Subscription.

General Terms

These General Terms apply to all of Customer's orders under this Agreement. Capitalized terms have the meanings given under "Definitions."

License to use Microsoft Products

- a. **License grant.** Products are licensed and not sold. Upon Microsoft's acceptance of each order and subject to Customer's compliance with this Agreement, Microsoft grants Customer a nonexclusive and limited license to use the Products ordered as provided in the applicable Use Rights and this Agreement. These licenses are solely for Customer's own use and business purposes and are nontransferable except as expressly permitted under this Agreement or applicable law.
- b. **Duration of licenses.** Licenses granted on a subscription basis or for a specified term expire at the end of the applicable subscription period or term unless renewed. Licenses granted for Products billed periodically based on metered usage continue as long as Customer continues to pay for usage of the Product. All other licenses become perpetual upon payment in full.
- c. **Applicable Use Rights.** The latest Use Rights, as updated from time to time, apply to the use of all Products, subject to the following exceptions. (1) For Products with metered usage-based pricing (e.g., metered Azure Services): Material adverse changes published after the start of a calendar month will apply beginning the following month. (2) For Versioned Software: Material adverse changes published after the date a Product is licensed will not apply to the use of that Product during that license or subscription term unless the changes are published with the release of a new version and a subscription customer chooses to update to that version. (3) For other Products: Material adverse changes published after the start of the subscription term will not apply during the subscription.
- d. **End Users.** Customer will control access to and use of the Products by End Users and is responsible for any use of the Products that does not comply with this Agreement.
- e. **Customer Eligibility.** Customer agrees that if it is purchasing academic, government or nonprofit offers, Customer meets the respective eligibility requirements (<https://aka.ms/eligibilitydefinition>). Microsoft reserves the right to verify eligibility and suspend product use if requirements are not met.
- f. **Affiliates.** Customer may order Products for use by its Affiliates. If it does, the licenses granted to Customer under this Agreement will apply to such Affiliates, but Customer will have the sole right to enforce this Agreement against Microsoft. Customer will remain responsible for all obligations under this Agreement and for its Affiliates' compliance with this Agreement.
- g. **Reservation of Rights.** Microsoft reserves all rights not expressly granted in this Agreement. No rights will be granted or implied by waiver or estoppel. Rights to access or use a Product on a device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.

- h. Restrictions.** Except as expressly permitted in this Agreement, or Product documentation, Customer must not (and is not licensed to): (1) reverse engineer, decompile, or disassemble any Product, or attempt to do so; (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; (3) work around any technical limitations in a Product or restrictions in Product documentation; (4) separate and run parts of the Product on more than one device; (5) upgrade or downgrade parts of the at different times; (6) transfer parts of a Product separately; or (7) distribute, sublicense, rent, lease, or lend any Product, in whole or in part, or use them to offer hosting services to a third party.
- h. License transfers and assignments.** Customer may only transfer fully-paid, perpetual licenses to (1) an Affiliate or (2) a third party solely in connection with the transfer of hardware to which, or employees to whom, the licenses have been assigned as part of (a) a divestiture of all or part of an Affiliate or (b) a merger involving Customer or an Affiliate. Upon such transfer, Customer must uninstall and discontinue using the licensed Product and render any copies unusable. Customer must notify Microsoft of a License transfer and provide the transferee a copy of these General Terms, the applicable Use Rights and any other documents necessary to show the scope, purpose and limitations of the licenses transferred. Attempted license transfers that do not comply with this section are void.

Non-Microsoft Products.

Non-Microsoft Products are provided under separate terms by the Publishers of such products. Customer will have an opportunity to review those terms prior to placing an order for a Non-Microsoft Product through a Microsoft online store or Online Service. Microsoft is not a party to the terms between Customer and the Publisher. Microsoft may provide Customer's contact information and transaction details to the Publisher. Microsoft makes no warranties and assumes no responsibility or liability whatsoever for Non-Microsoft Products. Customer is solely responsible and liable for its use of any Non-Microsoft Product.

Verifying compliance.

- a. Right to verify compliance.** Microsoft has the right, at its expense, to verify compliance on all use and distribution of products by Customer's and its Affiliates. To such end, Customer must keep records relating to all use and distribution of products. Verification will be conducted through an independent auditor retained by Microsoft, and Customer must provide, without undue delay, all necessary information, including visible access to systems running the Products and evidence of licenses for Products the Customer acquired from a third party, hosts, sublicenses, or distributes to third parties.
- b. Verifying process.** Microsoft will notify Customer at least thirty (30) calendar days in advance of its intent to verify Customer's compliance with the license terms for the Products Customer and its Affiliates use or distribute. The independent auditor is also subject to confidentiality obligation. This verification will take place during normal business hours and the auditor will make best efforts not to interfere with Customer's operations, during the course of the audit.
- c. Remedies for non-compliance.** If verification reveals any use of Products without applicable license rights, then within thirty (30) days, Customer must order sufficient licenses to cover its use. If such use or distribution is determined to be in excess of Customer's existing licenses by 5% or more of the audited environment(s) in the aggregate, then Customer must reimburse Microsoft for the costs Microsoft incurred in obtaining the verification and acquire the necessary additional licenses at 125% of the price, based on the then-current price list or the maximum allowed under applicable law, if less. Microsoft does not waive its rights to enforce this agreement or to protect its intellectual property by any other legal or contractual means.
- d. Customer self-audit.** Microsoft, at its sole discretion, may require Customer to conduct a self-audit, subject to the non-compliance remedies as set forth herein.

Privacy.

- a. **Customer's privacy.** Customer's privacy is important to Microsoft. Please read the Microsoft Privacy Statement (<https://go.microsoft.com/fwlink/?LinkId=521839>) as it describes the types of data Microsoft collects from Customer and Customer's devices ("Data"), how Microsoft uses that Data, and the legal bases Microsoft has to process that Data.

Confidentiality.

- a. **Confidential Information.** "Confidential Information" is non-public information that is designated "confidential" or that a reasonable person should understand is confidential, including, but not limited to, Customer Data, the terms of this Agreement, and Customer's account authentication credentials. Confidential Information does not include information that (1) becomes publicly available without a breach of a confidentiality obligation; (2) the receiving party received lawfully from another source without a confidentiality obligation; (3) is independently developed; or (4) is a comment or suggestion volunteered about the other party's business, products or services.
- b. **Protection of Confidential Information.** Each party will take reasonable steps to protect the other's Confidential Information and will use the other party's Confidential Information only for purposes of the parties' business relationship. Neither party will disclose Confidential Information to third parties, except to its Representatives, and then only on a need-to-know basis under nondisclosure obligations at least as protective as this Agreement. Each party remains responsible for the use of Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party. The Online Services Terms may provide additional terms regarding the disclosure and use of Customer Data.
- c. **Disclosure required by law.** A party may disclose the other's Confidential Information if required by law, but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order.
- d. **Residual information.** Neither party is required to restrict work assignments of its Representatives who have had access to Confidential Information. Each party agrees that the use of information retained in Representatives' unaided memories in the development or deployment of the parties' respective products or services does not create liability under this Agreement or trade secret law, and each party agrees to limit what it discloses to the other accordingly.
- e. **Duration of Confidentiality obligation.** These obligations apply (1) for Customer Data, until it is deleted from the Online Services; and (2) for all other Confidential Information, for a period of five years after a party receives the Confidential Information.

Product warranties.

a. Limited warranties and remedies.

- (1) **Online Services.** Microsoft warrants that each Online Service will perform in accordance with the applicable SLA during Customer's use. Customer's sole remedies for breach of this warranty are described in the SLA.
- (2) **Software.** Microsoft warrants that the Software version that is current at the time Customer acquired it will perform substantially as described in the applicable Product documentation for one year from the date Customer acquires a license for that Product. If it does not, and Customer notifies Microsoft within the warranty term, Microsoft will, at its option, (i) return the price Customer paid for the Software license or a prorated portion of the applicable Subscription fee for the Online Service (ii) repair or replace the Software.

The remedies above are Customer's sole remedies for breach of the warranties in this section. Customer waives any warranty claims not made during the warranty period.

- a. **Exclusions.** The warranties in this Agreement do not apply to problems caused by accident, abuse, or Use inconsistent with this Agreement or applicable documentation, including failure to meet minimum system requirements. These warranties do not apply to free, trial, preview, or prerelease products, services or features, including Previews or to components of Products that Customer is permitted to redistribute (each, a "Limited Offering").
- b. **Disclaimer.** Except for the limited warranties above and subject to applicable law, Microsoft provides no other warranties or conditions for Products and disclaims any other express, implied or statutory warranties for

Products, including warranties of quality, title, non-infringement, merchantability, and fitness for a particular purpose.

Defense of third-party claims.

The parties will defend each other against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if the defending party is promptly notified in writing of the claim and has the right to control the defense and any settlement of it. The party being defended must provide the defending party with all requested assistance, information, and authority. The defending party will reimburse the other party for reasonable out-of-pocket expenses it incurs in providing assistance. This section describes the parties' sole remedies and entire liability for such claims.

- a. By Microsoft.** Microsoft will defend Customer against any third-party claim to the extent it alleges that a Product made available by Microsoft for a fee and used within the scope of the license granted under this Agreement (unmodified from the form provided by Microsoft and not combined with anything else), misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party. If Microsoft is unable to resolve a claim of misappropriation or infringement, it may, at its option, either (1) modify or replace the Product with a functional equivalent or (2) terminate Customer's license and refund any license fees (less depreciation for perpetual licenses), including amounts paid in advance for unused consumption for any usage period after the termination date. Microsoft will not be liable for any claims or damages due to Customer's continued use of a Product after being notified to stop due to a third-party claim.
- b. By Customer.** To the extent permitted by applicable law, Customer will defend Microsoft and its Affiliates against any third-party claim to the extent it alleges that: (1) any Customer Data or Non-Microsoft Product hosted in an Online Service by Microsoft on Customer's behalf misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party; or (2) Customer's use of any Product, alone or in combination with anything else, violates the law or harms a third party.

Limitation of liability.

For each Product, each party's maximum, aggregate liability to the other under this Agreement is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the Products during the term of the applicable licenses, subject to the following:

- (i) **Subscriptions.** For Products ordered on a subscription basis, Microsoft's maximum liability to Customer for any incident giving rise to a claim will not exceed the amount Customer paid for the Product during the 12 months before the incident.
- (ii) **Free Products and distributable code.** For Product provided free of charge and code that Customer is authorized to redistribute to third parties without separate payment to Microsoft, Microsoft's liability is limited to direct damages finally awarded up to US\$5,000.
- (iii) **Exclusions.** In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, or loss of use, loss of profits, or interruption of business, however caused or on any theory of liability.
- (iv) **Exceptions.** No limitation or exclusions under this Agreement will apply to liability arising out of either party's (1) confidentiality obligations (except for liability related to Customer Data, which will remain subject to the limitations and exclusions above); (2) defense obligations; or (3) violation of the other party's intellectual property rights.

Partners.

- a. Selecting a Partner.** Customer may authorize a Partner to place orders on Customer's behalf and manage Customer's purchases by associating the Partner with its account. If the Partner's distribution right is terminated, Customer must

select an authorized replacement Partner or purchase directly from Microsoft. Partners and other third parties are not agents of Microsoft and are not authorized to enter into any agreement with Customer on behalf of Microsoft.

- b. Partner Administrator privileges and access to Customer Data.** If Customer purchases Online Services from a Partner or chooses to provide a Partner with administrator privileges, that Partner will be the primary administrator of the Online Services and will have administrative privileges and access to Customer Data and Administrator Data. Customer consents to Microsoft and its Affiliates providing the Partner with Customer Data and Administrator Data for purposes of provisioning, administering and supporting (as applicable) the Online Services. Partner may process such data according to the terms of Partner's agreement with Customer, and its privacy commitments may differ from Microsoft's. Customer appoints Partner as its agent for purposes of providing and receiving notices and other communications to and from Microsoft. Customer may terminate the Partner's administrative privileges at any time.
- c. Support and Professional Services.** Customer's Partner will provide details on support services available for Products purchased under this agreement. Support services may be performed by Partner or its designee, which in some cases may be Microsoft. If Customer purchases Professional Services under this agreement, the performance of those Professional Services will be subject to the terms and conditions in the Use Rights.

Pricing and payment.

If Customer orders from a Partner, the Partner will set Customer's pricing and payment terms for that order, and Customer will pay the amount due to the Partner. Pricing and payment terms related to orders placed by Customer directly with Microsoft are set by Microsoft, and Customer will pay the amount due as described in this section.

- a. Payment method.** Customer must provide a payment method or, if eligible, choose to be invoiced for purchases made on its account. By providing Microsoft with a payment method, Customer (1) consents to Microsoft's use of account information regarding the selected payment method provided by the issuing bank or applicable payment network; (2) represents that it is authorized to use that payment method and that any payment information it provides is true and accurate; (3) represents that the payment method was established and is used primarily for commercial purposes and not for personal, family or household use; and (4) authorizes Microsoft to charge Customer using that payment method for orders under this Agreement.
- b. Invoices.** Microsoft may invoice eligible Customers. Customer's ability to elect payment by invoice is subject to Microsoft's approval of Customer's financial condition. Customer authorizes Microsoft to obtain information about Customer's financial condition, which may include credit reports, to assess Customer's eligibility for invoicing. Unless the Customer's financial statements are publicly available, Customer may be required to provide their balance sheet, profit and loss and cash flow statements to Microsoft. Customer may be required to provide security in a form acceptable to Microsoft to be eligible for invoicing. Microsoft may withdraw Customer's eligibility at any time and for any reason. Customer must promptly notify Microsoft of any changes in its company name or location and of any significant changes in the ownership, structure, or operational activities of the organization.
- c. Invoice Payment terms.** Each invoice will identify the amounts payable by Customer to Microsoft for the period corresponding to the invoice. Customer will pay all amounts due within thirty (30) calendar days following the invoice date.
- d. Late Payment.** Microsoft may, at its option, assess a late fee on any payments to Microsoft that are more than fifteen (15) calendar days past due at a rate of two percent (2%) of the total amount payable, calculated and payable monthly, or the highest amount allowed by law, if less.
- e. Cancellation fee.** If a subscription permits early termination and Customer cancels the subscription before the end of the subscription or billing period, Customer may be charged a cancellation fee. For Online Services, Microsoft (1) will not provide a refund in connection with cancellation of a subscription if such cancellation occurs outside of the stated return period, and (2) reserves the right to invoice Customer for any future scheduled billings for any subscription cancelled in such a manner; cancellation terms may vary depending on the Product. Subject to Microsoft's discretion, Microsoft will provide a refund for certain Online Services subscriptions and will forego its right to invoice future scheduled billings.
- f. Recurring Payments.** For subscriptions that renew automatically, Customer authorizes Microsoft to charge Customer's payment method periodically for each subscription or billing period until the subscription is terminated. By authorizing recurring payments, Customer authorizes Microsoft to store Customer's payment details and process such payments as

either electronic debits or fund transfers, or as electronic drafts from the designated bank account (in the case of automated clearing house or similar debits), as charges to the designated card account (in the case of credit card or similar payments) (collectively, "Electronic Payments"). If any payment is returned unpaid or if any credit card or similar transaction is rejected or denied, Microsoft or its service providers reserve the right to collect any applicable return item, rejection or insufficient funds fee to the maximum extent permitted by applicable law and to process any such fees as an Electronic Payment or to invoice Customer for the amount due.

- g. Taxes.** Microsoft prices exclude applicable taxes unless identified as "tax inclusive" and similar. If any amounts are to be paid to Microsoft, Customer will also pay any applicable value added, goods and services, sales, gross receipts, or other transaction taxes, fees, charges, or surcharges, or any regulatory cost recovery surcharges or other transaction taxes, fees charges, or surcharges or any regulatory cost recovery surcharges or similar amounts that are owed under this Agreement and that Microsoft is permitted to collect from Customer. Customer will be responsible for any applicable stamp taxes and for all other taxes that it is legally obligated to pay including any taxes that arise on the distribution or provision of Products by Customer to its Affiliates. Microsoft will be responsible for all taxes based upon its net income, gross receipts taxes imposed in lieu of taxes on income or profits, and taxes on its property ownership.

If any taxes are required to be withheld on payments invoiced by Microsoft, Customer may deduct such taxes from the amount owed and pay them to the appropriate taxing authority, but only if Customer promptly provides Microsoft an official receipt for those withholdings and other documents reasonably requested to allow Microsoft to claim a foreign tax credit or refund. Customer will ensure that any taxes withheld are minimized to the extent possible under applicable law.

Term and termination.

- a. Term.** This Agreement is effective until terminated by a party, as described below.
- b. Termination without cause.** Either party may terminate this Agreement without cause on 60 days' notice. Termination without cause will not affect Customer's perpetual licenses, and licenses granted on a subscription basis will continue for the duration of the subscription period(s), subject to the terms of this Agreement.
- c. Termination for cause.** Without limiting other remedies it may have, either party may terminate this Agreement on 30 days' notice for material breach if the other party fails to cure the breach within the 30-day notice period. Upon such termination, the following will apply:
- (1) All licenses granted under this Agreement will terminate immediately except for fully-paid, perpetual licenses.
 - (2) All amounts due under any unpaid invoices shall become due and payable immediately. For metered Products billed periodically based on usage, Customer must immediately pay for unpaid usage as of the termination date.
 - (3) If Microsoft is in breach, Customer will receive a credit for any subscription fees, including amounts paid in advance for unused consumption for any usage period after the termination date.
- d. Suspension.** Microsoft may suspend use of an Online Service without terminating this Agreement during any period of material breach. Microsoft will give Customer notice before suspending an Online Service when reasonable. **Changes to Products.** Microsoft may modify, discontinue, or terminate a Product in any country or jurisdiction where there is any current or future government regulation, obligation, or other requirement, that (1) is not generally applicable to businesses operating there; and (2) either (i) presents a hardship for Microsoft to continue offering the Product without modification, or (ii) causes Microsoft to believe these terms or the Product may conflict with any such regulation, obligation, or requirement. If Microsoft terminates a subscription, Customer will receive, as its sole remedy, a credit for any subscription fees, including amounts paid in advance, for unused consumption for any usage period after the termination date.

Miscellaneous.

- a. Independent contractors.** The parties are independent contractors. Customer and Microsoft each may develop products independently without using the other's Confidential Information.
- b. Agreement not exclusive.** Customer is free to enter into agreements to license, use, and promote the products and services of others.
- c. Amendments.** Microsoft may modify this Agreement from time to time. Changes to the Use Rights will apply as provided in this Agreement. Changes to other terms will not apply until Customer accepts them. Microsoft may require Customer to accept revised or additional terms before processing a new order but the original terms will continue to govern Products acquired under prior orders.
- d. Assignment.** Either party may assign this Agreement to an Affiliate, but it must notify the other party in writing of the assignment. Customer consents to the assignment to an Affiliate or third party, without prior notice, of any rights Microsoft may have under this Agreement to receive payment and enforce Customer's payment obligations, and all assignees may further assign such rights without further consent. Any other proposed assignment of this Agreement must be approved by the non-assigning party in writing. Assignment will not relieve the assigning party of its obligations under the assigned Agreement. Any attempted assignment without required approval will be void.
- e. U.S. export.** Products are subject to U.S. export jurisdiction. Customer must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end use and destination restrictions by U.S. and other governments related to Microsoft products, services, and technologies.
- f. Severability.** If any part of this Agreement is held to be unenforceable, the rest of the Agreement will remain in full force and effect.
- g. Waiver.** Failure to enforce any provision of this Agreement will not constitute a waiver. Any waiver must be in writing and signed by the waiving party.
- h. No third-party beneficiaries.** This Agreement does not create any third-party beneficiary rights except as expressly provided by its terms.
- i. Survival.** All provisions survive termination of this Agreement except those requiring performance only during the term of the Agreement.
- j. Notices.** All notices must be in writing. Except for Notices of Dispute or notices relating to arbitration, notices to Microsoft must be sent to the following address and will be deemed received on the date received at that address:

Microsoft Corporation

Dept. 551, Volume Licensing

6100 Neil Road, Suite 210,

Reno, Nevada 89511-1137, USA

Notices to Customer will be sent to the individual at the address Customer identifies on its account as its contact for notices. Microsoft may send notices and other information to Customer by email or other electronic form and will be deemed received on the date received at such physical or email address. See paragraph below for where to send Notices of Dispute and other notices relating to arbitration.

- k. Applicable law and place to resolve disputes.** This Agreement will be governed by and construed in accordance with the laws of the State of Washington and federal laws of the United States. The 1980 United Nations Convention on Contracts for the International Sale of Goods and its related instruments will not apply to this Agreement.

l. Dispute resolution. When bringing any action arising under this Agreement, the parties agree to the following exclusive venues:

- (1) If Microsoft brings the action, the venue will be where Customer has its headquarters.
- (2) If Customer brings the action against Microsoft or any Microsoft Affiliate located outside of Europe, the venue will be the state or federal courts in King County, State of Washington, USA.
- (3) If Customer brings the action against Microsoft or any Microsoft Affiliate located in Europe, and not also against Microsoft or a Microsoft Affiliate located outside of Europe, the venue will be the Republic of Ireland.

The parties consent to personal jurisdiction in the agreed venue. This choice of venue does not prevent either party from seeking injunctive relief in any jurisdiction with respect to a violation of intellectual property rights or confidentiality obligations

m. Order of precedence. These General Terms will take precedence over any conflicting terms in other documents that are part of this Agreement that are not expressly resolved in those documents, except that conflicting terms in the Use Rights take precedence over these General Terms as to the applicable Products. Terms in the Online Services Terms take precedence over conflicting terms in the Product Terms. Terms in an amendment control over the amended document and any prior amendments concerning the same subject matter.

n. Microsoft Affiliates and contractors. Microsoft may perform its obligations under this Agreement through its Affiliates and use contractors to provide certain services. Microsoft remains responsible for their performance.

o. Government procurement rules. By accepting this agreement, Customer represents and warrants that (i) it has complied and will comply with all applicable government procurement laws and regulations; (ii) it is authorized to enter into this Agreement; and (iii) this Agreement satisfies all applicable procurement requirements.

Definitions.

"Administrator Data" means the information provided to Microsoft or its Affiliates during sign-up, purchase, or administration of Products.

"Affiliate" means any legal entity that controls, is controlled by, or is under common control with a party.

"Control" means ownership of more than a 50% interest of voting securities in an entity or the power to direct the management and policies of an entity.

"Confidential Information" is defined in the "Confidentiality" section.

"Customer" means the entity identified as such on the account associated with this Agreement.

"Customer Data" means all data, including all text, sound, software, image or video files that are provided to Microsoft or its Affiliates by, or on behalf of, Customer and its Affiliates through use of Online Services.

"End User" means any person Customer permits to use a Product or access Customer Data.

"Licensing Site" means <http://www.microsoft.com/licensing/contracts> or a successor site.

"Microsoft" means Microsoft Corporation.

"Non-Microsoft Product" means any third-party-branded software, data, service, website or product, unless incorporated by Microsoft in a Product.

"Online Services" means Microsoft-hosted services to which Customer subscribes under this Agreement. It does not include software and services provided under separate license terms.

"Online Services Terms" means the additional terms that apply to Customer's use of Online Services published on the Licensing Site and updated from time to time.

“Partner” means a company Microsoft has authorized to distribute Products to Customer.

“Personal Data” means any information relating to an identified or identifiable natural person.

“Product” means all Software and Online Services identified in the Product Terms that Microsoft offers under this Agreement, including previews, prerelease versions, updates, patches and bug fixes from Microsoft. Product availability may vary by region. “Product” does not include Non-Microsoft Products.

“Product Terms” means the document that provides information about Products available under this Agreement. The Product Terms document is published on the Licensing Site and is updated from time to time.

“Publisher” means a provider of a Non-Microsoft Product.

“Representatives” means a party’s employees, Affiliates, contractors, advisors and consultants.

“SLA” means Service Level Agreement, which specifies the minimum service level for the Online Services and is published on the Licensing Site.

“Software” means licensed copies of Microsoft software identified in the Product Terms. Software does not include Online Services, but Software may be part of an Online Service.

“use” means to copy, download, install, run, access, display, use or otherwise interact with.

“Use Rights” means the license terms and terms of service for each Product published on the Licensing Site and updated from time to time. The Use Rights include the Product-Specific License Terms, the License Model terms, the Universal License Terms, the Data Protection Terms, and the Other Legal Terms. The Use Rights supersede the terms of any end user license agreement that accompanies a Product.

Supplemental Government Community Cloud Terms.

If you are ordering a Government Community Cloud offering, the following terms apply:

- a. **Community requirements.** Customer certifies that it is a member of the Community and agrees to use Government Community Cloud Services solely in its capacity as a member of the Community and solely for the benefit of end users that are members of the Community. Customer must maintain its status as a member of the Community throughout the duration of the term for its Government Community Cloud Services. By maintaining or renewing its enrollment for Government Community Cloud Services, Customer certifies its continued membership of the Community. Use of Government Community Cloud Services by an entity that is not a member of the Community or to provide services to non-Community members is strictly prohibited. Customer acknowledges that only Community members may use Government Community Cloud Services.
- b. All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights and this Agreement.
- c. Disclaimer: Government Community Cloud Services are not designed to operate in the same domain as non-Government Community Cloud Services. Additionally, Office 365 GCC High cannot coexist in the same domain as commercial Office 365 or Office 365 GCC, each as described in the Office 365 Service Descriptions.
- d. **Use Rights for Government Community Cloud Services.** For Government Community Cloud Services, notwithstanding anything to the contrary in the Use Rights:
 - (i) Government Community Cloud Services will be offered only within the United States.
 - (ii) Additional terms set forth in the Use Rights, including without limitation to the Data Processing Terms section of the Online Services Terms (and the “Standard Contractual Clauses” that are incorporated by reference thereto) and all provisions in the Online Service Terms relating to the European Union General Data Protection Regulation, will not apply. In addition, the Government-specific portions of the Compliance Trust Center Page, and not the foregoing Data Processing Terms, describe the control standards and frameworks with which Government Community Cloud Services comply.
 - (iii) References to geographic areas in the Use Rights with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.
- e. **Definitions.**

“Community” means the community consisting of one or more of the following: (1) a Government, (2) a Customer using eligible Government Community Cloud Services to provide solutions to a Government or a qualified member of the Community, or (3) a Customer with Customer Data that is subject to Government regulations for which Customer determines and Microsoft agrees that the use of Government Community Cloud Services is appropriate to meet Customer’s regulatory requirements. Membership in the Community is ultimately at Microsoft’s discretion, which may vary by Government Community Cloud Service.

“Compliance Trust Center Page” means the compliance page of the Microsoft Trust Center, published by Microsoft at <https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx> or a successor site Microsoft later identifies.

“End User” means any person you permit to access Customer Data hosted in the Online Services or otherwise use the Online Services, or any user of a Customer Solution.

“Government Community Cloud Services” means Microsoft Online Services that are provisioned in Microsoft’s multi-tenant data centers for exclusive use by or for the Community and offered in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-145. Notwithstanding that other Microsoft Online Services that are Government Community Cloud Services are designated as such in the Use Rights and Product Terms.

“Online Services” means any of the Microsoft-hosted online services subscribed to by Customer under this agreement, including Government Community Cloud Services

ITAR Covered Services

This section applies to only the ITAR Covered Services, defined below, Customer orders under this Agreement. These terms only apply if Customer provides express notice to Microsoft of its intent to manage ITAR controlled data in the Customer Data in accordance with the directions provided here: <https://www.microsoft.com/en-us/trustcenter/compliance/itar>

Prerequisites:

- (i) Customer is responsible for ensuring that the prerequisites established or required by the ITAR are fulfilled prior to introducing ITAR-controlled data into the ITAR Covered Services.
 - (ii) Customer acknowledges that the ITAR Covered Services ordered under the Agreement enable End Users optionally to access and use a variety of additional resources, applications, or services that are (a) provided by third parties, or (b) provided by Microsoft subject to their own terms of use or privacy policies (collectively, for convenience, “add-ons”), as described in services documentation or in the portal through which your administrator(s) will manage and configure the ITAR Covered Services.
 - (iii) Customer is responsible for configuring the ITAR Covered Services and adopting and implementing such policies and practices for your End Users’ use of ITAR Covered Services, together with any add-ons, as you determine are appropriate to comply with the ITAR or other legal or regulatory requirements applicable to you and not generally applicable to Microsoft as an IT service provider. Customer acknowledges that only ITAR Covered Services will be delivered subject to the terms of this Section. Processing and storage of ITAR-controlled data in other services, including without limitation add-ons, is not supported. Without limiting the foregoing, data that Customer elects to provide to the Microsoft technical support organization, if any, or data provided by or on Customer’s behalf to Microsoft’s billing or commerce systems in connection with purchasing or ordering ITAR Covered Services, if any, is not subject to the provisions of this Section. Customer is solely responsible for ensuring that ITAR-controlled data is not included in support information or support case artifacts.
- a. **Special Terms.** The ITAR Covered Services are cloud services operated in a standardized manner with features and processes common across multiple customers. As part of Customer’s preparation to use the ITAR Covered Services for the storage, processing, or transmission of ITAR-controlled data, Customer should review applicable services documentation. Customer is solely responsible for determining the appropriate policies and practices needed for compliance with the ITAR.
 - b. **Personnel.** Microsoft personnel and contractors authorized by Microsoft to access Customer Data (that may include ITAR-controlled data) in the ITAR Covered Services, will be limited to U.S. persons, as that term is defined in the ITAR. Customer may also authorize other Microsoft personnel and contractors to access its Customer Data. Customer is solely responsible for ensuring any such authorization is permissible under the ITAR.
 - c. **Use of Subcontractors.** As set forth in the OST, Microsoft may hire subcontractors to provide services on its behalf. Any such subcontractors used in delivery of the ITAR Covered Services will be permitted to obtain Customer Data (that may include ITAR-controlled data) only to deliver the ITAR Covered Services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Storage and processing of Customer Data in the ITAR Covered Services is subject to Microsoft security controls at all times and, to the extent subcontractor personnel perform services in connection with ITAR Covered Services, they are obligated to follow Microsoft’s policies, including without limitation the geographic restrictions and controls selected by you in the configuration of the ITAR Covered Services.
 - d. **Notification.** The Security Incident handling process defined in the OST will apply to the ITAR Covered Services. In addition, the parties agree to the following:
 - (i) Customer acknowledges that effective investigation or mitigation of a Security Incident involving ITAR-controlled data may be dependent upon information or services configurations within Customer’s control. Accordingly, proper treatment of ITAR-controlled data will be a joint obligation between Microsoft and Customer. If Customer becomes aware of any unauthorized release of ITAR-controlled data to Microsoft or the use of a service other than the ITAR

Covered Service to store, process, or transmit ITAR-controlled data, Customer will promptly notify Microsoft of such event and provide reasonable assistance and information necessary for Microsoft to investigate and report such event.

- (ii) If, subsequent to notification of a Security Incident by Microsoft, Customer determines that ITAR-controlled data may have been subject to unauthorized inspection or disclosure, it is Customer's responsibility to notify the appropriate authorities of such event, or to notify impacted individuals, if Customer determines such notification is required under applicable law or regulation or Customer's internal policies.
- (iii) If either party determines it is necessary or prudent to make a voluntary disclosure to the Directorate of Defense Trade Controls regarding the treatment of ITAR-controlled data in the Online Services, such party will work in good faith to notify the other party of such voluntary disclosure prior to providing such voluntary disclosure. The parties will work together in good faith in the development and reporting of any such voluntary disclosure.

e. Conflicts. If there is any conflict between any provision in this Section and any provision in the Agreement, this Section shall control.

f. Definitions

"Defense Service" has the meaning provided in 22 C.F.R. § 120.

"End User" means an individual that accesses the ITAR Covered Services.

"ITAR" means the International Traffic in Arms Regulations, found at 22 C.F.R. §§ 120 - 130.

"ITAR-controlled data" means Customer Data that is regulated by the ITAR as Defense Articles or Defense Services.

"ITAR Covered Services" means, solely with respect to this agreement, the Azure Government services, listed as being in the scope for the ITAR at <https://www.microsoft.com/en-us/TrustCenter/Compliance/itar> or its successor site.

IRS 1075 Covered Services

This section applies only to the IRS 1075 Covered Services, defined below, Customer orders under this Agreement. These terms only apply if Customer provides express notice to Microsoft of its intent to order IRS 1075 Covered Services in accordance with the directions provided here: <https://www.microsoft.com/en-us/trustcenter/Compliance/IRS>

Customer Prerequisites:

- (i) Customer is responsible to ensure that the prerequisites established or required by IRS Publication 1075 are fulfilled prior to introducing FTI into the IRS 1075 Covered Services.
- (ii) Customer acknowledges that the IRS 1075 Covered Services enable End Users optionally to access and use a variety of additional resources, applications, or services that are (a) provided by third parties, or (b) provided by Microsoft subject to their own terms of use or privacy policies (collectively, for convenience, "add-ons"), as described in services documentation and/or in the portal through which Customer's administrator(s) will manage and configure the IRS 1075 Covered Services.
- (iii) Customer is responsible to review Online Services documentation, configure the services, and adopt and implement such policies and practices for Customer's End Users' use of IRS 1075 Covered Services, together with any add-ons, as Customer determines are appropriate in order for it to comply with IRS Publication 1075 or other legal or regulatory requirements applicable to Customer and not generally applicable to Microsoft as an IT service provider.
- (iv) Customer acknowledges that only IRS 1075 Covered Services will be delivered subject to the terms of this Section. No other services are supported by the terms of this Section. Without limiting the foregoing, data that Customer elects to provide to the Microsoft technical support organization ("Support Data"), if any, or data provided by or on your behalf to Microsoft's billing or commerce systems in connection with purchasing/ordering IRS 1075 Covered Services ("Billing Data"), if any, is not subject to the provisions of this Section. Customer is solely responsible for ensuring that FTI is not provided as Support Data or Billing Data.

a. IRS Publication 1075 Special Terms.

- (i) **IRS 1075 Covered Services.** The IRS 1075 Covered Services are cloud services operated in a standardized manner with features and processes common across multiple customers. As part of Customer's preparation to use the services for FTI, Customer should review applicable services documentation. Customer's compliance with IRS Publication 1075 will be dependent, in part, on Customer's configuration of the services and adoption and implementation of policies and practices for Customer's End Users' use of IRS 1075 Covered Services. Customer is solely responsible for determining the appropriate policies and practices needed for compliance with IRS Publication 1075.
- (ii) Microsoft and Customer have agreed that certain requirements of the Safeguarding Contract Language and IRS Publication 1075 will be fulfilled as set forth in the remainder of this section.

b. Background Checks. Notwithstanding anything to the contrary in the IRS Safeguarding Exhibit, all screened personnel authorized to have logical access to Customer Data (that may include FTI) in the IRS 1075 Covered Services will meet background check requirements equivalent to those defined in IRS Publication 1075.**c. Personnel Records and Training.** Microsoft will maintain a list of screened personnel authorized to access Customer Data (that may include FTI) in the IRS 1075 Covered Services, which will be available to you or to the IRS upon written request. Customer will treat Microsoft personnel personally identifiable information (PII) as Microsoft trade secret or security-sensitive information exempt from public disclosure to the maximum extent permitted by applicable law, and, if required to provide such Microsoft personnel PII to the IRS, will require the IRS to treat such personnel PII the same.**d. Training Records.** Microsoft will maintain security and disclosure awareness training records as required by IRS Publication 1075, which will be available to Customer upon written request.**e. Confidentiality Statement.** Microsoft will maintain a signed confidentiality statement, and will provide a copy for inspection upon request.**f. Cloud Computing Environment Requirements.** The IRS 1075 Covered Services are provided in accordance with the FedRAMP System Security Plan for the applicable services. Microsoft's compliance with controls required by IRS Publication 1075, including without limitation encryption and media sanitization controls, can be found in the applicable FedRAMP System Security Plan.**g. Use of Subcontractors.** Notwithstanding anything to the contrary in Attachment 1, as set forth in the OST, Microsoft may use subcontractors to provide services on its behalf. Any such subcontractors used in delivery of the IRS 1075 Covered Services will be permitted to obtain Customer Data (that may include FTI) only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Storage and processing of Customer Data in the IRS 1075 Covered Services is subject to Microsoft security controls at all times and, to the extent subcontractor personnel perform services in connection with IRS 1075 Covered Services, they are obligated to follow Microsoft's policies. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations. Subject to the preceding, Microsoft may employ subcontractor personnel in the capacity of augmenting existing staff, and understands IRS Publication 1075's reference to employees to include employees and subcontractors acting in the manner specified herein. It is the responsibility of the Customer to gain approval of the IRS for the use of all subcontractors.

Microsoft maintains a list of subcontractor companies who may potentially provide personnel authorized to access Customer Data in the Online Services, published for Azure branded services at <http://azure.microsoft.com/en-us/support/trust-center/>, or successor locations identified by Microsoft. Microsoft will update these websites at least 14 days before authorizing any new subcontractor to access Customer Data and provide Customer with a mechanism to obtain notice of that update.

h. Security Incident Notification. The Security Incident handling process defined in the OST will apply to the IRS 1075 Covered Services. In addition, the parties agree to the following:

- (i) Customer acknowledges that effective investigation or mitigation of a Security Incident may be dependent upon

information or services configurations within your control. Accordingly, compliance with IRS Publication 1075 Incident Response requirements will be a joint obligation between Microsoft and Customer.

- (ii) If, subsequent to notification from Microsoft of a Security Incident, Customer determines that FTI may have been subject to unauthorized inspection or disclosure, it is Customer's responsibility to notify the appropriate Agent-in-Charge, TIGTA (Treasury Inspector General for Tax Administration) and/or the IRS of a Security Incident, or to notify impacted individuals, if Customer determines this is required under IRS Publication 1075, other applicable law or regulation, or Customer's internal policies.

i. Customer Right to Inspect.

- (i) Audit by Customer. Customer will, (i) be provided quarterly access to information generated by Microsoft's regular monitoring of security, privacy, and operational controls in place to afford you an ongoing view into the effectiveness of such controls, (ii) be provided a report mapping compliance of the IRS 1075 Covered Services with NIST 800-53 or successor controls, (iii) upon request, be afforded the opportunity to communicate with Microsoft's subject matter experts for clarification of the reports identified above, and (iv) upon request, and at Customer's expense, be permitted to communicate with Microsoft's independent third party auditors involved in the preparation of audit reports. Notwithstanding anything to the contrary in the IRS Safeguarding Exhibit, Customer will use this information above to satisfy any inspection requirements under IRS Publication 1075 and agrees that the audit rights described in this section are the sole rights to be provided in full satisfaction of any audit that may otherwise be requested by the IRS or the Customer. Notwithstanding anything to the contrary in the IRS Safeguarding Exhibit, Microsoft will not grant any inspection rights to the IRS or access to Microsoft data centers or other facilities that may cause Microsoft to be non-compliant with its contractual obligations under FedRAMP, ISO 27001/27018, other US Government security related operations, or its internal security policies.
- (ii) Confidentiality of Audit Materials. Audit information provided by Microsoft to Customer will consist of highly confidential proprietary or trade secret information of Microsoft. Microsoft may request reasonable assurances, written or otherwise, that information will be maintained as confidential and/or trade secret information subject to this agreement prior to providing such information to Agency, and Agency will ensure Microsoft's audit information is afforded the highest level of confidentiality available under applicable law. Notwithstanding the foregoing, upon request and pursuant to appropriate confidentiality protections, Enrolled Affiliate shall be permitted to provide Microsoft's audit information described in Section i(i) to the IRS to satisfy the IRS inspection requirements under IRS Publication 1075.
- (iii) This Section i is in addition to compliance information available to Customer under the OST.

j. Definitions.

"End User" means an individual that accesses the IRS 1075 Covered Services.

"FTI" is defined as in IRS Publication 1075.

"IRS 1075 Covered Services" means Azure Government services listed as being in the scope for IRS 1075 at <http://azure.microsoft.com/support/trust-center/compliance/irs1075/> or its successor site. Without limitation, IRS 1075 Covered Services do not include any other separately branded Online Services.

"IRS Publication 1075" means the Internal Revenue Services (IRS) Publication 1075 effective September 30, 2016, including updates (if any) released by the IRS after signing the Agreement.

"Safeguarding Contract Language" or "IRS Safeguarding Exhibit" refers to Exhibit 7 of IRS Publication 1075.

Google Cloud Master General Terms

The Google Cloud Master Terms are comprised of the Google Cloud Master General Terms (“General Terms”), and all Services Schedules and Order Forms that are incorporated by reference into the Google Cloud Master Terms (collectively, the “Terms”).

Google Cloud Master General Terms

1. **Services.** After Customer and Reseller and/or Distributor complete and execute an Order Form, (a) Google will provide the Services to Customer in accordance with the Terms, including the SLAs, and (b) Customer may use the Services in accordance with the applicable Services Schedule.
2. **Customer Obligations.**
 - 2.1 **Consents.** Customer is responsible for any consents and notices required to permit (a) Customer’s use and receipt of the Services and (b) Google’s accessing, storing, and processing of data provided by Customer (including Customer Data, if applicable) under the Terms.
 - 2.2 **Compliance.** Customer will (a) ensure that Customer and its End Users’ use of the Services complies with the Terms, (b) use commercially reasonable efforts to prevent and terminate any unauthorized access or use of the Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Services of which Customer becomes aware.
 - 2.3 **Use Restrictions.** Customer will not, and will not allow End Users to, (a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any of the source code of the Services (except to the extent such restriction is expressly prohibited by applicable law); (b) sell, resell, sublicense, transfer, or distribute the Services; or (c) access or use the Services (i) in a manner intended to avoid incurring Fees; (ii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (iii) in a manner that breaches, or causes the breach of, Export Control Laws; or (iv) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA with Google’s Reseller or Distributor.
3. **RESERVED**
4. **Intellectual Property.**
 - 4.1 **Intellectual Property Rights.** Except as expressly described in the Terms, the Terms do not grant either party any rights, implied or otherwise, to the other’s content or Intellectual Property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data and Customer Applications, and Google retains all Intellectual Property Rights in the Services and Software.
 - 4.2 **Feedback.** At its option, Customer may provide feedback and suggestions about the Services to Google (“Feedback”). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer.
5. **Confidentiality.**
 - 5.1 **Confidentiality Obligations.** Subject to Section 5.2 (Disclosure of Confidential Information), and subject to

the Freedom of Information Act or similar state open records law, the recipient will use the other party's Confidential Information only to exercise its rights and fulfill its obligations under the Terms. The recipient will use reasonable care to protect against disclosure of the other party's Confidential Information to parties other than the recipient's employees, Affiliates, agents, or professional advisors ("Delegates") who need to know it and who have a legal obligation to keep it confidential. The recipient will ensure that its Delegates are also subject to the same non-disclosure and use obligations.

5.2 Disclosure of Confidential Information.

- (a) General. Regardless of any other provision in the Terms, the recipient and its Delegates may disclose the other party's Confidential Information (i) with the other party's written consent or (ii) in accordance with a Legal Process request, subject to Section 5.2(b) (Legal Process Notification).
- (b) Legal Process Notification. The recipient will use commercially reasonable efforts to notify the other party before disclosing that party's Confidential Information in accordance with Legal Process. Notice is not required before disclosure if the recipient is informed that (i) it is legally prohibited from giving notice or (ii) the Legal Process relates to exceptional circumstances involving danger of death or serious physical injury.
- (c) Opposition. The recipient will, and will ensure that its Delegates will, comply with the other party's reasonable requests to oppose disclosure of its Confidential Information.

- 6. **Marketing and Publicity.** Each party may use the other party's Brand Features in connection with these Terms as permitted in these Terms. Customer may state publicly that it is a Google customer and display Google Brand Features in accordance with the Trademark Guidelines. Customer and Google will work together on an announcement of Customer being a Google customer, which will take place on a mutually agreed upon date within 6 months of the Effective Date. Additionally, with prior written consent, the parties may engage in joint marketing activities such as customer testimonials, press engagements, public speaking events, and analyst interviews. A party may revoke the other party's right to use its Brand Features with 30 days' written notice. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features.

7. **RESERVED**

- 8. **Disclaimer.** Except as expressly provided for in these Terms, to the fullest extent permitted by applicable law, Google (a) does not make any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, fitness for a particular use, noninfringement, or error-free or uninterrupted use of the Services or Software and (b) makes no representation about content or information accessible through the Services. The Services are not intended to be used for High Risk Activities. Any use of the Services for High Risk Activities by Customer or its End Users will be at Customer's own risk, and Customer will be solely liable for the results of any failure of the Services when used for High Risk Activities.

9. **Indemnification.**

- 9.1 Google Indemnification Obligations. Google will defend Customer and its Affiliates participating under these Terms ("Customer Indemnified Parties"), and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that the Customer Indemnified Parties' use of Google Indemnified Materials infringes the third party's Intellectual Property Rights.
- 9.2 Customer Intellectual Property Infringement. If Google is damaged or becomes subject to a Third-Party Legal Proceeding as a result of Customer's infringement of any third-party intellectual property, Google

will pursue available remedies under applicable federal, state, or local law.

9.3 **Indemnification Exclusions.** Sections 9.1 (Google Indemnification Obligations) and 9.2 (Customer Intellectual Property infringement) will not apply to the extent the underlying allegation arises from (a) the Customer's or Google's breach of the Terms or (b) a combination of the Google Indemnified Materials or Customer Materials (as applicable) with materials not provided by Google or the Customer under the Terms, unless the combination is required by the Terms.

9.4 **Indemnification Conditions.** Sections 9.1 (Google Indemnification Obligations)) is conditioned on the following:

- (a) Customer must promptly notify Reseller who will promptly notify Google in writing of any allegation(s) that preceded the Third-Party Legal Proceeding and cooperate reasonably with Google to resolve the allegation(s) and Third-Party Legal Proceeding. If breach of this Section 9.4(a) prejudices the defense of the Third-Party Legal Proceeding, then Google's obligations under Section 9.1 (Google Indemnification Obligations) will be reduced in proportion to the prejudice.
- (b) Customer must tender sole control of the indemnified portion of the Third-Party Legal Proceeding to Google, subject to the following: (i) the Customer may appoint its own non-controlling counsel, at its own expense; and (ii) any settlement requiring the Customer to admit liability, pay money, or take (or refrain from taking) any action, will require the Customer's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

9.5 **Remedies.**

- (a) If Google reasonably believes the Services might infringe a third party's Intellectual Property Rights, then Google may, at its sole option and expense, (i) procure the right for Customer to continue using the Services, (ii) modify the Services to make them non-infringing without materially reducing their functionality, or (iii) replace the Services with a non-infringing, functionally equivalent alternative.
- (b) If Google does not believe the remedies in Section 9.5(a) are commercially reasonable, then Google may Suspend or terminate the impacted Services.

9.6 **Sole Rights and Obligations.** Without affecting either party's termination rights, this Section 9 (Indemnification) states the Customer's' sole and exclusive remedy under the Terms for any third-party allegations of Intellectual Property Rights infringement covered by this Section 9 (Indemnification).

10. **Liability.**

10.1 **Limited Liabilities.**

- (a) **To the extent permitted by applicable law and subject to Section 10.2 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Terms for any**
 - (i) indirect, consequential, special, incidental, or punitive damages or
 - (ii) lost revenues, profits, savings, or goodwill.
- (b) **Each party's total aggregate Liability for damages arising out of or relating to the Terms is limited to the Fees Customer paid under the applicable Services Schedule during the 12 month period before the event giving rise to Liability.**

10.2 Unlimited Liabilities. Nothing in these Terms excludes or limits either party's Liability for:

- (a) subject to Section 8 (Disclaimer), death, personal injury, or tangible personal property damage resulting from its negligence or the negligence of its employees or agents;
- (b) its fraud or fraudulent misrepresentation;
- (c) its obligations under Section 9 (Indemnification);
- (d) its infringement of the other party's Intellectual Property Rights;
- (e) its payment obligations; or
- (f) matters for which liability cannot be excluded or limited under applicable law.

11. Term and Termination.

- 11.1 Term. The Terms will remain in effect for the Term unless it expires or is terminated in accordance with the Reseller Agreement or Distributor Agreement.
- 11.2 Termination for Convenience. Subject to any financial commitments in an Order Form or addendum to the Terms, Customer may terminate the Terms or an Order Form for convenience with prior written notice to Reseller or Distributor.
- 11.3 RESERVED.
- 11.4 Effects of Termination. If the Terms terminate or expire, then all Services Schedules and Order Forms also terminate or expire. If an Order Form terminates or expires, then after that Order Form's termination or expiration effective date, (a) all rights and access to the Services under that Order Form will terminate (including access to Customer Data, if applicable), unless otherwise described in the applicable Services Schedule, and (b) Reseller or Distributor will send Customer a final invoice (if applicable) for payment obligations under that Order Form. Termination or expiration of one Order Form will not affect other Order Forms.
- 11.5 Survival. The following Sections will survive expiration or termination of the Terms: Section 4 (Intellectual Property), Section 5 (Confidentiality), Section 8 (Disclaimer), Section 9 (Indemnification), Section 10 (Liability), Section 11.4 (Effects of Termination), Section 12 (Miscellaneous), Section 13 (Definitions), and any additional sections specified in the applicable Services Schedule.

12. Miscellaneous.

- 12.1 Notices. Google will provide notices under the Terms to Customer by sending an email to the Notification Email Address. Customer will provide notices under the Terms to Google by sending an email to legal-notices@google.com. Notice will be treated as received when the email is sent. Customer is responsible for keeping its Notification Email Address current throughout the Term.
- 12.2 Emails. The parties may use emails to satisfy written approval and consent requirements under these Terms.
- 12.3 RESERVED.
- 12.4 RESERVED.
- 12.5 Force Majeure. Neither party will be liable for failure or delay in performance of its obligations to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war.

- 12.6 Subcontracting. Google may subcontract obligations under the Terms but will remain liable to Customer for any subcontracted obligations.
- 12.7 No Agency. These Terms do not create any agency, partnership, or joint venture between the parties.
- 12.8 No Waiver. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Terms.
- 12.9 Severability. If any part of the Terms are invalid, illegal, or unenforceable, the rest of the Terms will remain in effect.
- 12.10 No Third-Party Beneficiaries. The Terms do not confer any rights or benefits to any third party unless it expressly states that it does.
- 12.11 Equitable Relief. Nothing in the Terms will limit either party's ability to seek equitable relief.
- 12.12 RESERVED.
- 12.13 Amendments. Except as specifically described otherwise in the Terms, any amendment to the Terms must be in writing, expressly state that it is amending the Terms.
- 12.14 Independent Development. Nothing in the Terms will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs, or technology that are similar to the subject of the Terms, provided that the party does not breach its obligations under the Terms in doing so.
- 12.15 RESERVED.
- 12.16 Conflicting Terms. If there is a conflict among the documents that make up the Terms, then the documents will control in the following order: the applicable Order Form, the applicable Services Schedule, the General Terms, and the URL Terms.
- 12.17 RESERVED.
- 12.18 RESERVED.
- 12.19 RESERVED.
- 12.20 Headers. Headings and captions used in the Terms are for reference purposes only and will not have any effect on the interpretation of the Terms.

13. Definitions.

"Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.

"AUP" means Google's acceptable use policy as defined in the applicable Services Schedule.

"BAA" or "Business Associate Agreement" is an amendment to the Customer's Reseller Agreement or Distributor Agreement, and covers the handling of Protected Health Information (as defined in HIPAA).

"Brand Features" means each party's trade names, trademarks, logos, domain names, and other distinctive

brand features.

“Confidential Information” means information that one party (or an Affiliate) discloses to the other party under these Terms, and that is marked as confidential or would normally be considered confidential information under the circumstances. Customer Data is Customer’s Confidential Information. Confidential Information does not include information that is independently developed by the recipient, is shared with the recipient by a third party without confidentiality obligations, or is or becomes public through no fault of the recipient.

“Control” means control of greater than 50% of the voting rights or equity interests of a party.

“Customer Application” has the meaning described in the Services Schedule. “Customer Data” has the meaning described in the Services Schedule (if applicable).

“Distributor” means an entity authorized by Google to distribute the Services to a Reseller for resale to federal, state, or local government entities of the United States (or representatives of such entities).

“Distributor Agreement” means, if applicable, the separate agreement between Customer and Distributor regarding the Services. The Distributor Agreement is independent of and outside the scope of these Terms.

“Customer Materials” has the meaning described in the applicable Services Schedule.

“End User” or “Customer End User” means an individual that Customer permits to use the Services or a Customer Application.

“Export Control Laws” means all applicable export and re-export control laws and regulations, including (i) the Export Administration Regulations (“EAR”) maintained by the U.S. Department of Commerce, (ii) trade and economic sanctions maintained by the U.S. Treasury Department’s Office of Foreign Assets Control, and (iii) the International Traffic in Arms Regulations (“ITAR”) maintained by the U.S. Department of State.

“Fees” means the product of the amount of Services used or ordered by Customer multiplied by the Prices, plus any applicable Taxes. Fees will be described in Customer’s Reseller Agreement or Distributor Agreement.

“Google Indemnified Materials” has the meaning described in the applicable Services Schedule.

“High Risk Activities” means activities where the failure of the Services could lead to death, serious personal injury, or severe environmental or property damage.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time, and any regulations issued under it.

“Including” means including but not limited to.

“Indemnified Liabilities” means any (i) settlement amounts approved by the Customer, and (ii) damages and costs finally awarded against the Customer by a court of competent jurisdiction.

“Intellectual Property” or “IP” means anything protectable by an Intellectual Property Right.

“Intellectual Property Right(s)” means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

“Legal Process” means an information disclosure request made under law, governmental regulation, court order,

subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure, or similar process.

“Liability” means any liability, whether under contract, tort (including negligence), or otherwise, regardless of whether foreseeable or contemplated by the parties.

“Notification Email Address” has the meaning described in the applicable Services Schedule.

“Order Form” has the meaning described in the applicable Services Schedule or, as applicable, an Order Form provided by a Reseller or Distributor.

“Order Term” means the period of time starting on the Services Start Date for the Services and continuing for the period indicated on the Order Form unless terminated in accordance with the Terms.

“Reseller Agreement” means the separate agreement between Customer and Reseller regarding the Services. The Reseller Agreement is independent of and outside the scope of these Terms.

“Reseller” means, if applicable, the authorized non-Affiliate third party reseller that sells Google Services through a Distributor to Customer.

“Prices” means those prices listed in the applicable Reseller Agreement or Distributor Agreement.

“Service Level Agreement” or “SLA” has the meaning described in the Services Schedule.

“Services” has the meaning described in the applicable Services Schedule.

“Services Schedule(s)” means a schedule to the Terms with terms that apply only to the services and software (if applicable) described in that schedule.

“Services Start Date” means either the start date described in the Order Form or, if none is specified in the Order Form, the date Google makes the Services available to Customer.

“Software” has the meaning described in the Services Schedule (if applicable).

“Suspend” or “Suspension” means disabling access to or use of the Services or components of the Services.

“Term” means the Term as described in the applicable Reseller Agreement or Distributor Agreement.

“Third-Party Legal Proceeding” means any formal legal proceeding filed by an unaffiliated third party before a court or government tribunal (including any appellate proceeding).

“Trademark Guidelines” means Google’s Brand Terms and Conditions described at <https://www.google.com/permissions/trademark/brand-terms.html>.

“URL” means a uniform resource locator address to a site on the internet.

“URL Terms” has the meaning described in the Services Schedule.

“Use Restrictions” means the restrictions in Section 2.3 (Use Restrictions) of these General Terms and any additional restrictions on the use of Services described in a section entitled “Additional Use Restrictions” in the applicable Services Schedule.

Google Cloud Master Terms

Google Cloud Platform Services Schedule

This Google Cloud Platform Services Schedule (the “Services Schedule”) supplements and is incorporated by reference into the Google Cloud Master Terms. This Services Schedule applies solely to the services and software described in this Services Schedule and is effective so long as there is an active Order Form. Terms defined in the General Terms apply to this Services Schedule.

1. Using the Services.

- 1.1 Admin Console. Google (or Reseller or Distributor) will provide Customer an Account to access the Admin Console through which Customer may manage its use of the Services. Customer may make Customer Applications available to End Users. Customer is responsible for (a) maintaining the confidentiality and security of the Account and associated passwords and (b) any use of the Account.
- 1.2 Ceasing Services Use. Customer may stop using the Services at any time.
- 1.3 Additional Use Restrictions. Unless otherwise permitted in the GCP Service Specific Terms, Customer will not use, and will not allow End Users to use, the Services or any Customer Application to operate or enable any telecommunications service or to place or receive calls from any public switched telephone network.
- 1.4 Resold Customer.
 - (a) Reseller and Distributor have the ability to suspend the Customer’s Account. Customer is solely responsible for: (i) any access by Reseller and Distributor to Customer’s Account or Customer’s End User Accounts; (ii) any suspension by Reseller or Distributor of Customer’s or Customer’s End User’s Services, and (ii) defining in the Reseller Agreement or Distributor Agreement, as applicable, any rights or obligations as between Reseller and Customer, or Distributor and Customer, with respect to the Services;
 - (b) Google may share Customer Confidential Information with Reseller and/or Distributor as a Delegate subject to General Terms Section 5.1 (Confidentiality Obligations);
 - (c) Google will not be liable in any manner whatsoever to Customer arising out of Reseller’s and/or Distributor’s suspension of the Customer’s Account or Reseller’s and/or Distributor’s access to the Customer’s and Customer End User’s Account(s).

2. Data Processing and Security.

- 2.1 Use of Customer Data. Google will only access or use Customer Data to provide the Services ordered by Customer and will not use it for any other Google products, services, or advertising.
- 2.2 Data Processing and Security Terms. The Data Processing and Security Terms are provided to Customer by Reseller or Distributor

2.3 Federal Risk and Authorization Management Program (FedRAMP).

- (a) The following Google Cloud Platform Services received a FedRAMP High Provisional Authority to Operate (ATO) from the Joint Authorization Board (JAB): **Compute:** Compute Engine, App Engine, Google Kubernetes Engine **Storage:** Cloud Storage, Persistent Disk **Security:** Cloud HSM, Cloud Key Management Service **Data Analytics:** BigQuery, Cloud Dataproc, Cloud Pub/Sub **Databases:** Cloud Bigtable, Cloud Dataflow, Cloud Firestore, Cloud Memorystore, Cloud Spanner, Cloud SQL **Developer Tools:** Container Registry.
- (b) The following Google Cloud Platform Services received a FedRAMP Moderate Provisional ATO from the Joint Authorization Board (JAB): **Compute:** Compute Engine, App Engine, Cloud Functions, Google Kubernetes Engine **Storage:** Cloud Storage, Persistent Disk **Networking:** Cloud Armor, Cloud CDN, Cloud DNS, CloudLoad Balancing, Virtual Private Cloud (VPC) **Security:** Cloud Data Loss Prevention API, Cloud HSM, Cloud Identity & Access Management, Cloud Identity-Aware Proxy, Cloud Key Management Service, Cloud Security Scanner, Resource Manager **Management Tools:** Cloud Billing API, Cloud Console, Cloud Console Mobile App, Cloud Deployment Manager, Cloud Shell, Google Cloud Platform Marketplace, Service Consumer Management API, Service Control, Service Management API, Stackdriver Debugger, Stackdriver Error Reporting, Stackdriver Logging, Stackdriver Profiler, Stackdriver Trace **Data Analytics:** BigQuery, Cloud Dataflow, CloudDatalab, Cloud Dataproc, Cloud Pub/Sub, Cloud Talent Solution, Google Genomics **Databases:** Cloud Bigtable, Cloud Datastore, Cloud Firestore, Cloud Memorystore, Cloud Spanner, Cloud SQL **Migration:** BigQuery Data Transfer Service, Cloud Storage Transfer Service **AI/Machine Learning:** Cloud AutoML Natural Language, Cloud AutoML Translation, Cloud AutoML Vision, Cloud Machine Learning Engine, Cloud Natural Language API, Cloud Speech-to-Text, Cloud Text-to-Speech, Cloud Translation API, Cloud Video Intelligence API, Cloud Vision API, Dialogflow Enterprise Edition **Developer Tools:** Cloud Build, Cloud SDK, Cloud Source Repositories, Container Registry **API Management:** Cloud Endpoints **Internet of Things (IoT):** Cloud IoT Core
- (c) Google, Reseller, and Distributor are not liable for any damages, claims, or causes of action that arise from the loss or failure to maintain the ATO. Customer's sole remedy in connection with the loss or failure to maintain the ATO will be the Customer's ability to terminate use of Provider's Google Cloud Platform Service.

3. **Additional Payment Terms.**

- 3.1 **Usage and Invoicing.** Customer will pay all Fees for the Services and GCP Technical Support Services. Google's measurement tools will be used to determine Customer's usage of the Services. Each invoice, which may be generated by Reseller or Distributor, will include data in sufficient detail to allow Customer to validate the Services purchased and associated Fees.
- 3.2 **RESERVED.**
- 3.3 **RESERVED.**

4. **Updates to Services and Terms.**

4.1 **Changes to Services.**

- (a) **Limitations on Changes.** Google may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services.
- (b) **Discontinuance.** Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality), and at least 36 months for any Key Service (or associated material functionality), unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

4.2 **Changes to Terms.** Google may update the URL Terms, provided the updates do not (a) result in a material degradation of the overall security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing and Security Terms, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms.

4.3 **Permitted Changes.** Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to new or pre-general availability Services or functionality.

5. **Temporary Suspension.**

5.1 **Services Suspension.** Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Customer or any End User's use of the Services does not comply with the AUP, and it is not cured following notice from Google.

5.2 **Limitations on Services Suspensions.** If Google Suspends Services, then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

6. **Technical Support.** If Customer has purchased Enterprise Support or Role-Based Support, Google will provide GCP Technical Support Services to Customer during the Order Term in accordance with the GCP Technical Support Services Guidelines. Customer is responsible for the technical support of its Customer Applications and Projects. Customer acknowledges and agrees that Reseller and/or Distributor may disclose Customer Data to Google as may be reasonably required in order for Reseller and/or Distributor to handle any support issues that Customer may escalate to or via Reseller and/or Distributor.

7. **Copyright.** Google provides information to help copyright holders manage their intellectual property online, but Google cannot determine whether something is being used legally without input from the copyright holders. Google will respond to notices of alleged copyright infringement and may terminate repeat infringers in appropriate circumstances as required to maintain safe harbor for online service providers under the U.S. Digital

Millennium Copyright Act. If Customer believes a person or entity is infringing Customer's or its End User's copyrights and would like to notify Google, Customer can find information about submitting notices, and Google's policy about responding to notices, at <http://www.google.com/dmca.html>.

8. Software.

8.1 Provision of Software. Google may make Software available to Customer, including third-party software. Customer may choose to use the Software in connection with Customer's use of the Services. Some Software may be subject to third-party license terms, which Google will provide to Customer.

8.2 Ceasing Software Use. If the Customer's Reseller Agreement or Distributor Agreement terminates, or the Google Cloud Platform Order Form terminates or expires, then Customer will stop using the Software.

9. **Benchmarking.** Customer may only publicly disclose (directly or through a third party) the results of any comparative or compatibility testing, benchmarking, or evaluation (each, a "Test") of the Services, if the disclosure includes all information reasonably necessary for Google or a third party to replicate the Test. If Customer conducts, or directs a third party to conduct, a Test of the Services and publicly discloses the results directly or through a third party, then Google (or a Google-directed third party) may conduct Tests of any publicly available cloud products or services provided by Customer and publicly disclose the results of any such Test (which disclosure will include all information necessary for Customer or a third party to replicate the Test).

10. **Survival.** The following sections of this Services Schedule will survive expiration or termination of this Services Schedule: Section 9 (Benchmarking) and Section 12 (Additional Definitions).

11. **Termination of Previous Agreements.** If Google and Customer have previously entered into a Google Cloud Platform License Agreement, then that agreement will terminate on the Services Start Date, and these terms will govern the provision and use of the Services going forward.

12. Additional Definitions.

"Account" means Customer's Google Cloud Platform account.

"Admin Console" means the online console(s) and tool(s) provided by Google to Customer for administering the Services under this Services Schedule.

"AUP" means the then-current acceptable use policy for the Services described at <https://cloud.google.com/terms/aup/>.

"Customer Application" means a software program that Customer creates or hosts using the Services.

"Customer Data" means data provided to Google by Customer or End Users through the Services under the Account, and data that Customer or End Users derive from that data through their use

of the Services.

“Customer Materials” means Customer Data, Customer Brand Features, Customer Applications, and Projects.

“Data Processing and Security Terms” means the then-current terms describing data processing and security obligations with respect to Customer Data, as described at <https://cloud.google.com/terms/data-processing-terms/partner/>. For purposes of these Terms, references to “Partner Data” in the Data Processing and Security Terms shall mean “Customer Data”.

“GCP Service Specific Terms” means the then-current terms specific to one or more Services or Software described at <https://cloud.google.com/cloud/terms/service-terms>.

“GCP Technical Support Services” or “TSS” means the then-current technical support service provided, if applicable, by Google to Customer under the GCP Technical Support Services Guidelines.

“GCP Technical Support Services Guidelines” or “TSS Guidelines” means the then-current Google Cloud Platform support service guidelines described at <https://cloud.google.com/terms/tssg/>.

“Google Indemnified Materials” means Google’s technology used to provide the Services and Google’s Brand Features.

“Key Services” means the then-current list of Services described at <https://cloud.google.com/terms/key-services>.

“Notification Email Address” means the email address(es) designated by Customer in the Admin Console.

“Order Form” means an order form issued by Reseller and/or Distributor and executed by Customer specifying the Services Google will provide to Customer as described in this Services Schedule.

“Prices” means those prices listed in the applicable Reseller Agreement or Distributor Agreement.

“Project” means a grouping of Services configured by Customer via the Admin Console.

“Services” means the then-current services described at <https://cloud.google.com/terms/services>.

“SLA” means the then-current service level agreements described at <https://cloud.google.com/terms/sla/>.

“Software” means any downloadable tools, software development kits, or other such computer

software provided by Google for use in connection with the Services, and any updates Google may make to such Software from time to time.

“URL Terms” means, as applicable, the AUP, Data Processing and Security Terms, GCP Service Specific Terms, GCP Technical Support Serv