MicroStrategy Cloud Environment

SERVICE GUIDE

UPDATE PUBLISHED MAY 2024

Copyright Information

Trademark Information

The following are either trademarks or registered trademarks of MicroStrategy Incorporated or its affiliates in the United States and certain other countries:

Dossier, Enterprise Semantic Graph, Expert.Now, Hyper.Now, HyperIntelligence, HyperMobile, HyperVision, HyperWeb, Intelligent Enterprise, MicroStrategy, MicroStrategy 2019, MicroStrategy 2020, MicroStrategy 2021, MicroStrategy Analyst Pass, MicroStrategy Architect, MicroStrategy Architect Pass, MicroStrategy Auto, MicroStrategy Cloud, MicroStrategy Cloud Intelligence, MicroStrategy Command Manager, MicroStrategy Communicator, MicroStrategy Consulting, MicroStrategy Desktop, MicroStrategy Developer, MicroStrategy Distribution Services, MicroStrategy Education, MicroStrategy Embedded Intelligence, MicroStrategy Enterprise Manager, MicroStrategy Federated Analytics, MicroStrategy Geospatial Services, MicroStrategy Identity, MicroStrategy Identity Manager, MicroStrategy Identity Server, MicroStrategy Insights, MicroStrategy Integrity Manager, MicroStrategy Intelligence Server, MicroStrategy Library, MicroStrategy Mobile, MicroStrategy Narrowcast Server, MicroStrategy ONE, MicroStrategy Object Manager, MicroStrategy Office, MicroStrategy OLAP Services, MicroStrategy Parallel Relational In-Memory Engine (MicroStrategy PRIME), MicroStrategy R Integration, MicroStrategy Report Services, MicroStrategy SDK, MicroStrategy System Manager, MicroStrategy Transaction Services, MicroStrategy Usher, MicroStrategy Web, MicroStrategy Workstation, MicroStrategy World, Usher, and Zero-Click Intelligence.

The following design marks are either trademarks or registered trademarks of MicroStrategy Incorporated or its affiliates in the United States and certain other countries:

Other product and company names mentioned herein may be the trademarks of their respective owners.

Specifications subject to change without notice. MicroStrategy is not responsible for errors or omissions. MicroStrategy makes no warranties or commitments concerning the availability of future products or versions that may be planned or under development.

TABLE OF CONTENTS

1. Overview

The MicroStrategy Cloud Environment service ("MCE" or "MCE Service") is a platform-as-a-service ("PaaS") offering that MicroStrategy manages on its customers' behalf in an Amazon Web Services, Microsoft Azure, or Google Cloud Platform environment that includes access to, collectively, (a) the "Cloud Platform" version of MicroStrategy software products (an optimized version of the MicroStrategy software platform built specifically for deployment in an Amazon Web Services, Microsoft Azure, or Google Cloud Platform environment) licensed by the customer; (b) Cloud Support, as described below; and (c) Cloud Architecture, as described below. MicroStrategy's PaaS delivery model is designed to allow businesses to consume the MicroStrategy Analytics and Mobility platform in a single tenant architecture (unless otherwise described in Section 6 MicroStrategy AI Product) without the need to deploy and manage the underlying infrastructure.

MCE offers a distributed compute architecture using cloud-native services provided by either Microsoft Azure, Amazon Web Services or Google Cloud Platform. As this technology evolves, MicroStrategy continually incorporates new services that allow for increased availability, security, or performance to ensure the latest architecture is available to our customers. At the core of the solution are MicroStrategy Analytics and Mobility, a secure, scalable, and resilient business intelligence enterprise application platform.

MCE also includes the elements needed to operate, access, and manage the intelligence architecture. Users are provisioned with their own dedicated intelligence architecture based on a reference architecture. Once provisioned, users can develop, tailor, and manage the application components to meet their respective needs.

Based on this operating model, customers administer and control the Analytics and Mobility solution while MicroStrategy maintains the supporting cloud-based infrastructure.

2. Cloud Support

As an MCE Service customer, you will receive "Cloud Application Support" ("Cloud Support") in which our Cloud Support engineers will provide ongoing support over your MCE Service term to assist in maximizing the performance and agility—and minimizing the cost— of your MicroStrategy Cloud Platform deployment. Cloud Support includes environment configuration (setting up customer accounts in a selected region and CIDR for VPC/VNETs/Subnets), enterprise data warehouse integration (including modifying the MicroStrategy configuration for data warehouse connections and opening any connectivity for external data warehouses), authentication (SSO/OIDC), and application integration. Additionally, Standard Support for the Cloud Platform version of MicroStrategy Products is provided with the licenses for such Products pursuant to your contract with MicroStrategy and our Technical Support Policies and Procedures, except that all MCE customers are entitled to four Support Liaisons (as defined in the Technical Support Policies and Procedures). MicroStrategy Cloud Elite Support is sold to MCE Service customers as an add-on offering to standard Cloud Support. A subscription to Cloud Elite Support provides MCE Service customers, among other benefits, with enhanced initial response times for P1 and P2 issues, four additional Support Liaisons (eight total), weekly case management meetings, and customizable system alerts. MicroStrategy's Cloud Support Offerings are detailed below in Appendix A.

If a production outage issue occurs, MicroStrategy reserves the right to fix the issue on behalf of the customer without pre-authorization. If a support issue is logged and determined through the diagnosis

that the Root Cause Analysis (RCA) that the stated issue is due to a customer-specific customization of the MicroStrategy application, the Cloud Support team will provide the customer with available options to resolve the issue. These solutions may require the purchase of MicroStrategy Professional Services for additional assistance depending on the complexity of the issue.

3. Cloud Architecture

The Cloud Architecture offered as part of the MCE Service is an optimized reference architecture providing enterprise-grade data design and governance, and consists of (a) the Cloud Architecture components required to run your PaaS environment, configured through either the Single-Instance Architecture, or a cluster High-Availability MCE Architecture constructs detailed below, and (b) Cloud Environment Support, the support services and components needed to successfully run the infrastructure and architecture components of the MCE Service offering.

3.1 Cloud Infrastructure

Our MCE Service offers single tenant platform architectures built based on industry best practices for security, compliance, and availability. All offerings are fully managed cloud environments with 24 x 7 availability and separate metadata servers, load balancers, firewalls, data egress, and other services to ensure ease of use. This cloud infrastructure ("Additional PaaS Components") is available in several configurations, as described below:

A. The cloud infrastructure provided with the Cloud Architecture - Tier 1 operating environment (designated on an order as "Cloud Platform for AWS-Tier 1-MCE" or "Cloud Platform for Azure-Tier 1-MCE" or "Cloud Platform for GCP – Tier 1 – MCE") includes the following components:

- one (1) production instance with up to 256 GB RAM;
- one (1) non-production instance with up to 128 GB RAM; and
- one (1) non-production windows instance with up to 32 GB RAM

B. The cloud infrastructure provided with the Cloud Architecture - Tier 2 operating environment (designated on an order as "Cloud Platform for AWS-Tier 2-MCE" or "Cloud Platform for Azure-Tier 2-MCE" or "Cloud Platform for GCP – Tier 2 – MCE") includes the following components:

- two (2) production instances (clustered) with up to 512 GB RAM;
- one (1) non-production instance with up to 256 GB RAM; and
- one (1) non-production windows instance with up to 32 GB RAM.

C. The cloud infrastructure provided with the Cloud Architecture - Tier 3 operating environment (designated on an order as "Cloud Platform for AWS-Tier 3-MCE" or "Cloud Platform for Azure-Tier 3-MCE" or "Cloud Platform for GCP – Tier 3 – MCE") includes the following components:

- two (2) production instances (clustered) with up to 1 TB RAM each;
- two (2) non-production instances (clustered) OR two (2) non-production instances (non-clustered) with up to 512 GB RAM each; and
- two (2) non-production windows instances with up to 64 GB RAM each.

D. The cloud infrastructure provided with the Cloud Architecture - Tier 4 operating environment (designated on an order as "Cloud Platform for AWS-Tier 4-MCE" or "Cloud Platform for Azure-Tier 4-MCE" or "Cloud Platform for GCP – Tier 4 – MCE") includes the following components:

- two (2) production instances (clustered) with up to 2 TB RAM each;

- two (2) non-production instances (clustered) OR two (2) non-production instances (non-clustered) with up to 1 TB RAM each; and
- two (2) non-production windows instances with up to 64 GB RAM each.

E. Cloud Architecture - Standard offering (designated on an order as "Cloud Architecture - AWS" or "Cloud Architecture - Azure) includes the following components:

- one (1) production node with up to 512 GB RAM;
- one (1) non-production development node with up to 64 GB RAM; and
- one (1) non-production utility node with up to 32 GB RAM.

Additional nodes are also available to purchase, through the execution of an order, as an add-on to this offering. Each additional node purchased is for use in either production or non-production environments and includes up to 512 GB RAM. A customer may purchase additional nodes to create a clustered production instance (inclusive of a high-performance file system) or for use as separate, standalone environments for quality assurance or development.

F. The Cloud Architecture - Small offering (designated on an order as "Cloud Architecture - AWS Small" or "Cloud Architecture – Azure Small") is available for purchase by certain small to medium sized customers with less complex requirements and includes the following components:

- one (1) production node with up to 128 GB RAM; and
- one (1) non-production utility node with up to 16 GB RAM.

G. The Cloud Architecture - GCP standard offering (designated on an order as "Cloud Architecture – GCP") includes the following components:

- one (1) node with up to 640 GB RAM; and
- one (1) non-production utility node with up to 32 GB RAM.

Additional GCP nodes are also available to purchase, through the execution of an order, as an add-on to this offering. Each additional node purchased includes up to 640 GB RAM. A customer may purchase additional nodes to create a clustered production instance (inclusive of a high-performance file system) or for use as separate, standalone environments for quality assurance or development.

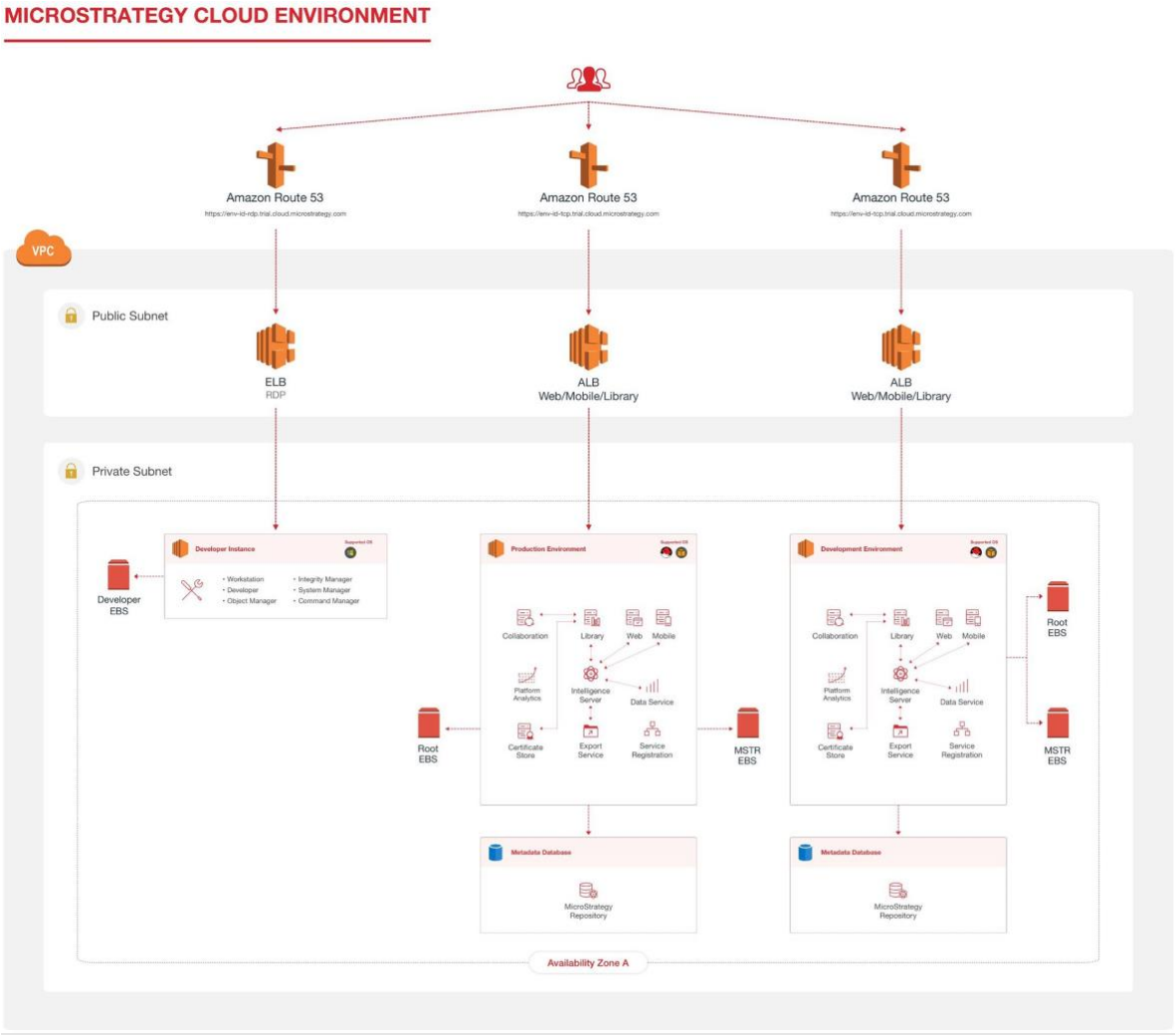
H. The Cloud Architecture – GCP Small offering (designated on an order as "Cloud Architecture – GCP Small") is available for purchase by certain small to medium sized customers with less complex requirements and includes the following components:

- one (1) node with up to 128 GB RAM; and
- one (1) non-production utility node with up to 16 GB RAM.

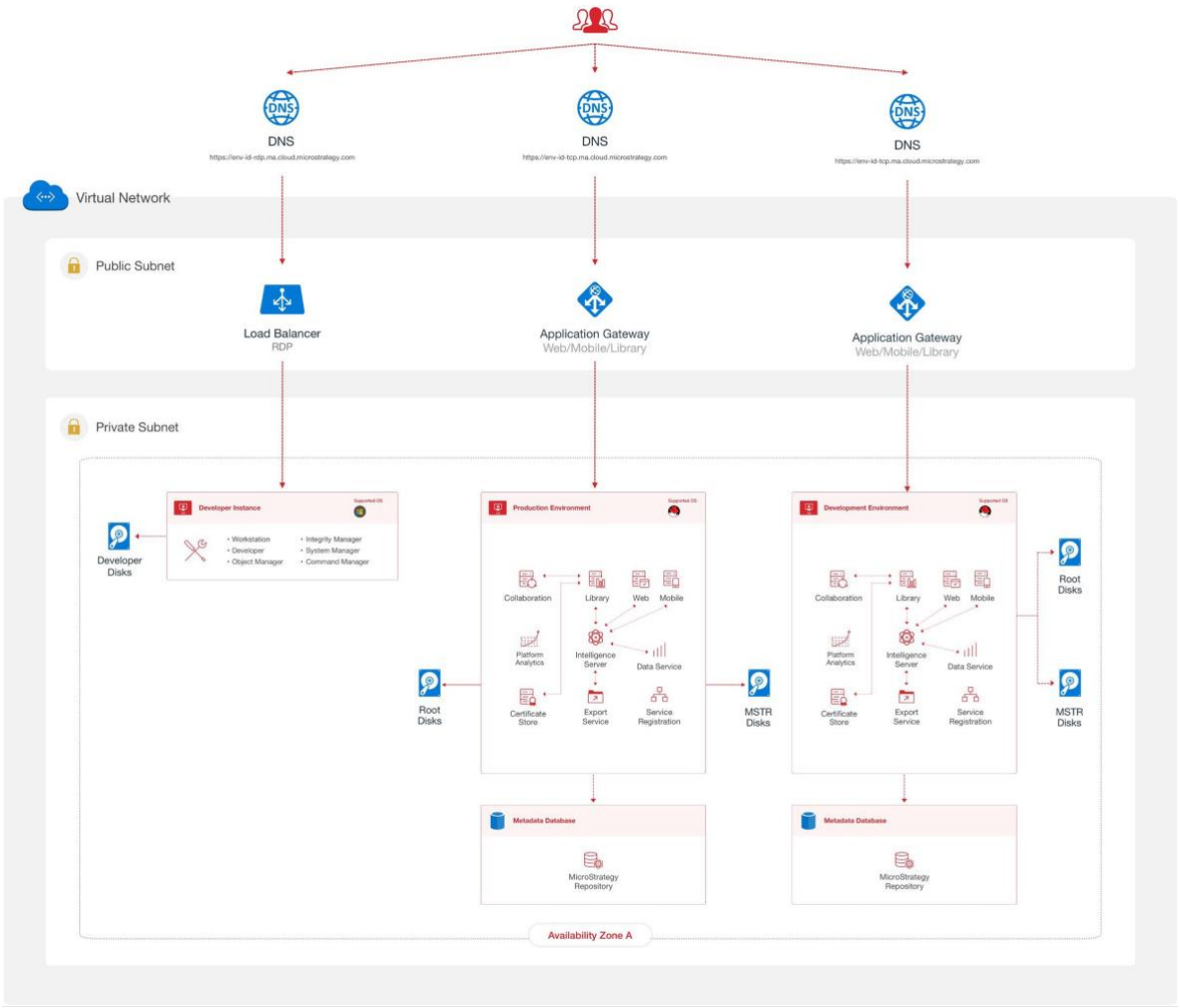
These offerings are procured on your behalf from Microsoft Azure, Amazon Web Services, or Google Cloud Platform to host the MicroStrategy Cloud Platform in a MicroStrategy Cloud Environment and will be operated out of a mutually determined data center location. As part of these additional PaaS components, we will also provide you Cloud Environment Support for your instances, as further described in this Guide, which includes support of your MicroStrategy Cloud Platform managed by MicroStrategy experts in the MicroStrategy Cloud Environment. Such support also includes 24x7x365 system monitoring and alerting, daily backups for streamlined disaster recovery, updates and quarterly system reviews, and annual compliance checks and security certifications. Additionally, all MCE customers will receive up to 1 TB per month of data egress at no additional charge. As part of the MCE quarterly service review, we will advise you if your monthly data egress usage is close to or exceeds 1 TB for each MCE environment.

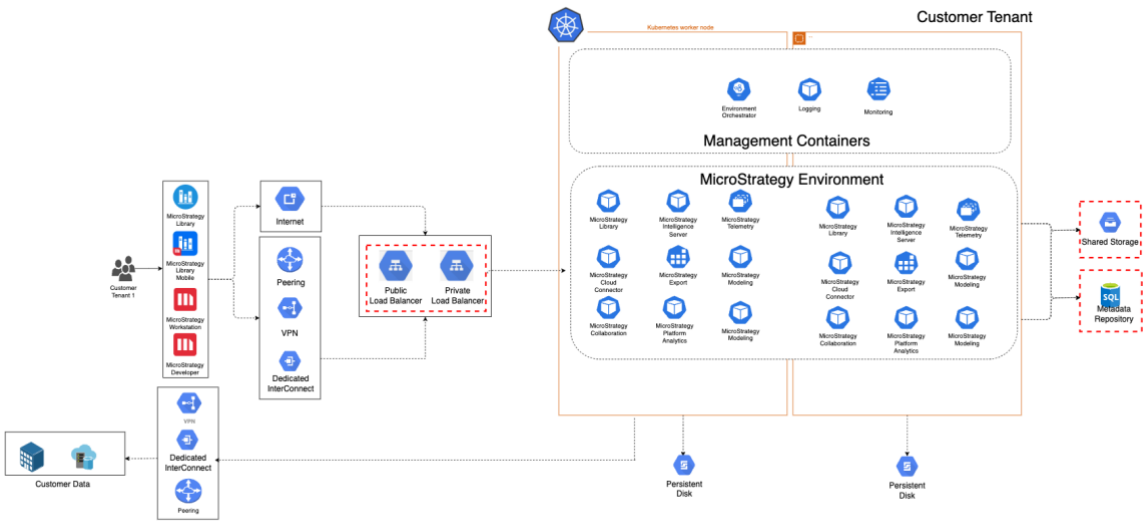
3.1.1 MCE Architecture

Customers who purchase either the AWS, Azure, or GCP Cloud Architecture – Standard or Cloud Architecture – Tier 1 offering of MicroStrategy's MCE Architecture will receive one Production instance, one non-Production instance, and one Windows instance from either Microsoft Azure or Amazon Web Services or GCP, as demonstrated in the diagrams below. Each instance consists of a single server for MicroStrategy Intelligence Server, Web, Library, Mobile, and Collaboration. There is also a database for the MicroStrategy metadata, statistics, insights, and collaboration services. The MCE Architecture is built to scale to thousands of end users.



MICROSTRATEGY CLOUD ENVIRONMENT





3.1.2 High-Availability MCE Architecture

MicroStrategy's High-Availability MCE Architecture consists of a clustered Cloud Architecture spanned across multiple Availability Zones. MicroStrategy Metadata database is also highly available through a multi-Availability Zone architecture offered by cloud service providers. The High-Availability MCE Architecture is included in the Cloud Architecture Tier 2, Tier 3, and Tier 4 offerings. MCE customers may move to the next available Tier if additional non-production instances are required, listed in Section 3.1.

3.2 Cloud Environment Support

As part of the Cloud Architecture, MicroStrategy will provide Cloud Environment Support to you by maintaining your environments for the total number of instances purchased as part of an MCE Service subscription, including the following:

3.2.1 Service Availability

Service availability for production instances is 24x7 and for non-production instances is a minimum of 12x5 in the customer's local time zone. These parameters may be changed based upon mutual agreement.

3.2.2 Root Cause Analysis (RCA)

For production outages, an RCA can be requested by the customer. Customers will receive the RCA report within ten (10) business days of the request.

Cloud Support will cover all aspects regarding diagnosis of the RCA. It may also cover product defects, security updates, operating system updates, and changes. As noted in Section 2, if an RCA determines an issue to be created by a customer-specific customization, MicroStrategy will provide options outside of Cloud Support, such as Professional Services engagements, to remedy the issue.

3.2.3 24/7 Cloud Support Hotline

For Production instance outages where system restoration is paramount, a global cloud team is mobilized for prompt resolution. The MicroStrategy Cloud team functions around the clock to support customers and maintain service SLA's.

3.2.4 24/7 Monitoring and Alerting

Key system parameters are monitored for all production and non-production instances. MicroStrategy has alerts on CPU utilization, RAM utilization, disk space, application-specific performance counters, VPN Tunnel, and ODBC warehouse sources monitoring. As part of MicroStrategy's Cloud Elite Support Offering customers are eligible to receive custom alerts. System performance is logged over time to give the customer and Cloud Support team the ability to maintain a performant cloud platform.

3.2.5 Backups

Daily backups are performed for all customer systems, including system state and metadata. By default, MCE customers will have a seven (7) day backup retention period, a thirty (30) day extended backup cycle encompassing metadata, and a monthly backup archive for the preceding eleven (11) months. All backups are inclusive of metadata, data storage services, cubes, caches, images, and plugins. Please reach out to your Account Executive for additional cost estimates if you have additional backup requirements.

3.2.6 Platform Analytics

MicroStrategy Platform Analytics is set up for all MicroStrategy customers on MCE and maintained to allow for instant access to system performance metrics. MicroStrategy will monitor the MCE Service-based data repository and/or cube memory requirement of the Platform Analytics database. In the event the space availability is less than 20% of the allocated storage, after receiving the customer's consent, MicroStrategy will purge older data from the MCE Service-based Platform Analytics database in 30-day increments until the disk availability is below the 80% capacity threshold. The amount of data that the customer chooses to keep may have a corresponding cost to the customer. Contact your Account team for a cost estimate to modify the MCE Service, including increases to the data repository and/or cube memory requirements.

3.2.7 Maintenance

Maintenance windows are scheduled monthly to allow for third-party security updates to be applied to the MCE platform. During these scheduled interruptions, the MCE systems may be unable to transmit and receive data through the provided services. Customers should plan to create a process that includes the pause and restart of applications, rescheduling subscriptions, and including but not limited to, related data load routines. When it is necessary to execute emergency maintenance procedures, MicroStrategy will notify customer-specific support liaisons via email as early as possible—identifying the nature of the emergency and the planned date and time of execution. Customers will normally receive a minimum of two weeks' advance notification for planned maintenance windows. However, if emergency maintenance work is required, we will use commercially reasonable efforts to give 24-to-48-hour notice before applying a remedy. MCE customers are required to adhere to their monthly maintenance window. If the assigned window is not suitable, please contact your Cloud Technical Account Manager (CTM).

3.2.8 Quarterly Service Reviews

The assigned designated Cloud Technical Account Manager (CTM) for your MCE will conduct the Quarterly Service Reviews (QSR) with the business and technical contacts on a quarterly cadence. This may include the overview of system resources and recommendations based on observed trends.

3.2.9 Infrastructure Availability

The MCE Service is architected to withstand the failure of an individual service to maintain availability. For clustered environments, this is achieved by utilizing underlying application features and building

on best practices. MicroStrategy Cloud also utilizes the advantages of Availability Zones ("AZ") in AWS, Azure, and GCP.

3.2.10 Fail-Over

Standard fail-over routines allow for backups and system state data with storage spanning AZs. The use of multiple AZs for clustered production environments creates a physical separation of data between the machines storing production and backup environments. MicroStrategy provides an RPO (Recovery Point Objective) of 24 hours with an RTO (Recovery Time Objective) of 48 hours upon an Availability Zone failure.

3.2.11 Disaster Recovery

MicroStrategy's MCE offering does not provide region failover in its standard offering. However, customers do have the option to purchase Disaster Recovery (DR) as an add-on to the standard offering at an additional cost. MicroStrategy recommends having a secondary data warehouse site available for failover purposes when considering a disaster recovery purchase. MicroStrategy provides the below options for DR:

- Hot-Cold: Customer environment in the failover Region has been provisioned and shut down and is only started when the disaster occurs in the primary region. This provides an estimated targeted RPO of 24 hours and an RTO of 6 hours.
- Hot-Warm: Customer environment in the failover Region has been provisioned and goes through a daily Metadata refresh. The environment is shut down after the refresh. This provides a targeted RPO of 24 hours and an RTO of 4 hours.

3.2.12 Updates and Upgrades

MicroStrategy is committed to providing the latest updates with security fixes, therefore all customers are required to take advantage of the fixes and new features. For each Product license, we will deliver to you every Quarter, at no charge and at your request, an Update and or Upgrade as part of the Technical Support Services subscription. Major upgrades are completed in a free parallel environment for up to 30 days to allow for customer testing. Updates may not include new separately marketed products. Customers requiring longer than 30 days to complete the upgrade should contact their Account Executive.

Your CTM will work with you each quarter to schedule the updates. These updates are seamless and carry over all customizations in your MicroStrategy environment. The customer is responsible for ensuring SDK Mobile apps are recompiled to comply with newer versions of MicroStrategy. Customers are also encouraged to perform regression testing on the updated environment along with data validation and testing other custom workflows.

3.2.13 Roles and Responsibilities

The RACI Table below in Appendix B highlights the roles and responsibilities of customers and MicroStrategy. Please note that some responsibility relies on Cloud service providers and, therefore, MicroStrategy will comply with cloud providers Service Level Agreement for service availability.

3.2.14 Non-Migrated MicroStrategy Components

Stated below are MicroStrategy components that will not be hosted in cloud. Customers are highly encouraged to move away from legacy components and leverage newer and modern replacement of such tools:

- MicroStrategy Narrowcast Server replaced with Distribution services
- MicroStrategy Enterprise Manager replaced with Platform Analytics

The following items below are supported only for connectivity to MCE. MicroStrategy will not host them in the Cloud. These solutions may require additional assistance from MicroStrategy Professional Services.

- IIS web server to support MDX
- Customizations not in plugin form

Distribution Services

All MicroStrategy Cloud customers are required to use their own SMTP server for delivery of email and history list subscriptions. File subscriptions are pushed to AWS S3 bucket or Azure BLOB Storage or Google Cloud Storage provided to the customer as part of the MCE infrastructure to all customers. Customers may pull file subscriptions from the storage locations provided during the on-boarding process with their CTMs.

3.2.15 MCE Migration Licensing

Two additional licenses are provided for Cloud operations and maintenance. These accounts are the 'mstr_svc' and 'Axx-administrator' or 'Cxx-administrator' or 'Gxx-administrator'. MSTR User should always be disabled, not deleted. MicroStrategy Cloud Team will enable MSTR user when necessary, i.e. Updates and Upgrades.

3.2.16 AI Capabilities

The "MicroStrategy AI," and "MicroStrategy AI User" SKUs provide artificial intelligence capabilities as a part of your MCE Service ("AI Capabilities").

AI Capabilities are designed to accommodate various user roles, and provide AI-assisted data exploration, automated dashboard design processes, SQL generation tools, and ML-based visualization methods. The AI Capabilities within the framework of the MicroStrategy analytics platform augment the platform's data processing and presentation capabilities. The use of AI Capabilities may have limitations which impact the effectiveness, quality and/or accuracy of output from your MCE Service and should not replace human decision-making. You remain responsible for judgments, decisions, and actions you make or take based on the output of your MCE Service.

Notwithstanding anything to the contrary, we may provide AI Capabilities to you from an environment that is different from the operating environment specified on your MCE Service order. You may not perform any penetration testing on the artificial intelligence service powering the AI Capabilities.

Consumption-Based Licensing and Auto-Replenishment of the MicroStrategy AI SKU
For each MicroStrategy AI SKU quantity you license, you may consume up to twenty thousand (20,000) Questions (as defined below) for a period of up to twelve (12) months beginning on the order effective date and, in the case of a replenishment, from the beginning of the replenishment effective date (each period, a "Use Period"). Unconsumed Questions are automatically forfeited at the earlier of (a) the end of the Use Period, or (b) termination or expiry of the MCE Service term, and do not carry over to any subsequent Use Periods. Upon the earlier of the expiration of the Use Period or the full consumption of 20,000 Questions, we will automatically replenish your right to consume an additional 20,000 Questions for each licensed MicroStrategy AI SKU quantity for a subsequent Use Period, each at the then current list price for such MicroStrategy, unless you provide written notice to us that you desire not to auto-replenish (a) at least ninety (90) days before the expiration of the then current Use Period, or (b) before 18,000 Questions have been consumed, whichever occurs first.

MicroStrategy AI is otherwise non- cancelable by you, and non-refundable. For the avoidance of doubt, the foregoing does not apply to the licensing of the MicroStrategy AI User SKU, which is licensed on a named user basis, with no limit on the number of questions.
Customers purchasing the MicroStrategy AI SKU will have access to Platform Analytics which will include your usage in its reporting.

One "Question" is defined as any input action taken while using the MicroStrategy AI SKU. Below are examples of a Question:

- Auto Answers (multiple consumption options):
    - one action submitted to MicroStrategy's Auto chatbot that returns a response constitutes consumption of one Question.

- one click on auto-populated suggestions below MicroStrategy's Auto chatbot input box constitutes consumption of one Question.
- any subsequent selection(s) of the recommended data analysis constitutes consumption of an additional Question.

- Auto SQL:
  - one action submitted to MicroStrategy's Auto chatbot that returns a response constitutes consumption of one Question.
- Auto Dashboard (multiple consumption options):
  - one action submitted to MicroStrategy's Auto chatbot that returns a response constitutes consumption of one Question.
  - one click on auto-populated suggestions below MicroStrategy's Auto chatbot input box constitutes consumption of one Question.
  - any subsequent selection(s) of the recommended data analysis constitutes consumption of an additional Question.

3.2.17 Security

Various security tools are employed to perform penetration testing and remediation, system event logging, and vulnerability management. The MCE Service maintains a high security posture in accordance with the following security standards:

Service Organization Controls (SSAE-18)*

SSAE-18 is the service organization auditing standard maintained by the AICPA. It evaluates Service Organization Controls over the security, availability, and processing integrity of a system and the confidentiality and privacy of the information processed by the system. Our MCE Service maintains a SOC2 Type 2 report.

Health Insurance Portability and Accountability Act (HIPAA)

Controls designed to protect health information.

Payment Card Industry Data Security Standards (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information. MCE maintains a SAQ-D for Service Providers.

International Organization for Standardization (ISO 27001-2)*

International Organization for Standardization (ISO 27001-2) is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance.

*MicroStrategy is in the process of receiving certification for the above security standards on Google Cloud Platform. Certifications are anticipated to be completed in 2024.

3.2.18 MCE Security Scans

MicroStrategy will conduct a security review on all custom components provided by the customers such as plugins, drivers, etc. Customer is responsible for remediation of all security findings.

3.2.19 Cloud Shared Services Components

As part of the MCE Service's platform architecture and in support of the Cloud Environment, we incorporate third-party solutions to assist in the management, deployment, and security of the

infrastructure, and to complete operational tasks. These include management and detection response solutions, cloud security posture management solutions, application/infrastructure monitoring, alerting and on call management solutions, and workflow and continuous integration tools.

4 Service Availability

MCE offers a service level agreement of 99.9% for clustered production environments and 99% service level for single instance non-clustered production environments. Availability is calculated per calendar month as follows:

$$\left[\left(\frac{\text{Total Minutes} * \#\text{ of Production Instances} - \text{Unavailability}}{\text{Total Minutes} * \#\text{ of Production Instances}} \right) * 100 \right]$$

4.1 Service Definition

"Total Minutes": the total number of minutes in a calendar month.

"Production Instance": an MCE Intelligence Architecture that users are running in production, in support of an operational business process.

"Unavailability": for each Production Instance, the total number of minutes in a calendar month during which (1) the Production Instance(s) has no external connectivity; (2) the Production Instance(s) has external connectivity but is unable to process requests (i.e., has attached volumes that perform zero read- write IO, with pending IO in the queue); or (3) all connection requests made by any component of the Production Instance(s) fail for at least five consecutive minutes. "Unavailability" does not include minutes when the MCE is unavailable due to issues related to applications built on the MicroStrategy software platform, including project, report, and document issues; migration problems related to user design; ETL application problems; improper database logical design and code issues; downtime related to scheduled maintenance; downtime experienced as a result of user activity; general internet unavailability; and other factors out of MicroStrategy's reasonable control.

"Total Unavailability": the aggregate unavailability across all Production Instances.

For any partial calendar month during which customers subscribe to the MCE, availability will be calculated based on the entire calendar month, not just the portion for which they subscribed.

4.2 Service Remedies

If the availability standard of 99.9% (for clustered Production Instances) and 99% (for non-clustered Production Instance) is not met in any given calendar month, customers may be eligible for a Service Credit, according to the definitions below. Each Service Credit will be calculated as a percentage of the total fees paid by customers for the MCE Service, managed by MicroStrategy within the calendar month that a Service Credit has been accrued. This is the exclusive remedy available to customers in the event MicroStrategy fails to comply with the service level requirements set forth in the availability designed in Section 4.

4.3 Service Credits

Clustered Production Instance:

- Availability less than 99.9% but equal to or greater than 99.84%: 1% Service Credit
- Availability less than 99.84% but equal to or greater than 99.74%: 3% Service Credit
- Availability less than 99.74% but equal to or greater than 95.03%: 5% Service Credit
- Availability less than 95.03%: 7% Service Credit

Non-Clustered Production Instance:

- Availability less than 99% but equal to or greater than 98.84%: 1% Service Credit
- Availability less than 98.84% but equal to or greater than 98.74%: 3% Service Credit
- Availability less than 98.74% but equal to or greater than 94.03%: 5% Service Credit
- Availability less than 94.03%: 7% Service Credit

4.4 Service Credits Procedure

To receive a Service Credit, customers must submit a MicroStrategy case on or before the 15th day of the calendar month following the calendar month in which the Service Credit allegedly accrues that includes the following information: (a)the words "SLA Credit Request" in the "Case Summary/ Error Message" field; (b) a detailed description of the event(s) that resulted in unavailability; (c) the dates, times, and duration of the unavailability; (d) the affected system or component ID(s) provided to customers by MicroStrategy during onboarding and Intelligence Architecture delivery activities; and (e) a detailed description of the actions taken by users to resolve the unavailability. Once MicroStrategy receives this claim, MicroStrategy will evaluate the information provided and any other information relevant to determining the cause of the Unavailability (including, for example, information regarding the availability performance of the Intelligence Architecture, third-party software or services, dependencies on customer-hosted or subscribed software or services, operating system, and software components of the MCE). Thereafter, MicroStrategy will determine in good faith whether a Service Credit has accrued and will notify customers of its decision. If MicroStrategy determines that a Service Credit has accrued, then at its discretion, it will either (1) apply the Service Credit to the next MCE Service invoice sent or (2) extend the MCE Service Term for a period commensurate to the Service Credit amount. Customers may not offset any fees owed to MicroStrategy with Service Credits.

5 Terms Applicable to Processing Personal Data

This Section 5 will apply only to the extent there is no other executed agreement in place regarding the same subject between MicroStrategy and the customer ("Customer"), including any order(s) and/or a master agreement between the customer and MicroStrategy (collectively, the "Governing Agreement"), and shall be considered a Data Processing Addendum (DPA). Except as amended by this DPA, the Governing Agreement will remain in full force and effect.

5.1 Definitions

"Applicable Data Protection Law" means all applicable laws and regulations where these apply to MicroStrategy, its group and third parties who may be utilized in respect of the performance of the MCE Service relating to the processing of personal data and privacy, including, without limitation, the General Data Protection Regulation (EU) 2016/679, the United Kingdom General Data Protection Regulation, and U.S. Data Privacy Laws (defined below) The terms "Controller," "Commissioner," "Business," "Processor," "Data Subject," "Supervisory Authority," "process," "processing," and

"personal data" shall be construed in accordance with their meanings as defined under Applicable Data Protection Law.

"Customer Group" means Customer and any affiliate, subsidiary, subsidiary undertaking and holding company of Customer (acting as a Controller) accessing or using the MCE Service on Customer's behalf or through Customer's systems or any other third party who is permitted to use the MCE Service pursuant to the Governing Agreement between Customer and MicroStrategy, but who has not signed its own Order Form with MicroStrategy.

"EU Standard Contractual Clauses" means Module 3 those clauses comprised within the European Commission Decision (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries under General Data Protection Regulation (EU) 2016/679, as may be updated, supplemented, or replaced from time to time under Applicable Data Protection Law and which are incorporated by reference herein forming part of this DPA and a copy of which can be accessed at www.microstrategy.com/en/legal/contract-hub, subject to the provisions of Section 5.5 below.

"EU-US Data Privacy Framework" means the European Commission implementing decision of 10 July 2023 pursuant to the General Data Protection Regulation.

"International Transfer" means a transfer of personal data from a country within the European Economic Area (EEA) or Switzerland or the United Kingdom (both countries not in the EEA or the EU) to a country or territory not recognized by the European Commission, Switzerland or the United Kingdom as providing an adequate level of protection for personal data or subject to any requirement to take additional steps to adequately protect personal data.

"MCE Service" means the MicroStrategy Cloud Environment service, a platform-as-a-service offering that we manage on the Customer's behalf in an Amazon Web Services, Microsoft Azure, or Google Cloud Platform environment that includes access to, collectively: (a) the "Cloud Platform" version of our Products (an optimized version of the MicroStrategy software platform built specifically for deployment in an Amazon Web Services, Microsoft Azure, or Google Cloud Platform environment) licensed by the Customer; (b) Cloud Support; and (c) the Additional PaaS Components (as defined above in Section 3.1 Cloud Infrastructure) for your use with such Products.

"Sub-Processor" means any third party appointed by MicroStrategy to process personal data.

"U.S. Data Privacy Laws" means any and all applicable U.S. privacy law or U.S. state privacy statutes and regulations relating to the protection of Personal Data, whether in existence as of the effective date or promulgated thereafter, as amended or superseded, including without limitation the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020, and all regulations issued thereunder ("CCPA"); the Virginia Consumer Data Protection Act of 2021, Va. Code Ann. §§ 59.1-571 et seq. ("VCDPA"), as effective January 1, 2023; the Colorado Privacy Act of 2021, Colo. Rev. Stat. §§ 6-1-1301 et seq. ("CPA"), as will be operative beginning July 1, 2023; the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, Conn. Gen. Stat. §§ 42-515 et seq. ("CTDPA"), as will be operative beginning July 1, 2023; the Utah Consumer Privacy Act of 2021, Utah Code Ann. §§ 13-61-101 et seq. ("UCPA"), as will be operative beginning December 31, 2023; the Texas Data Privacy and Security Act, Tex. Bus. & Com. Code §§ 541 et seq. ("TDPSA"), as will be operative beginning July 1, 2024; the Florida Digital Bill of Rights, Fla. Stat. §§ 501.701 et seq. ("FDBR"), as will be operative beginning July 1, 2024; the Montana Consumer Data Privacy Act, 2023 SB 384 ("MCDPA"), as will be operative beginning October 1, 2024; the Iowa Consumer Data Protection Act, Iowa Code §§ 715D et seq. ("ICDPA"), as will be operative beginning January 1, 2025; the Tennessee Information Protection Act, Tennessee Code Ann. §§ 47-18-3201 et seq. ("TIPA"), as will be operative beginning July 1, 2025; and the Indiana Consumer Data

Privacy Act, Indiana Code §§ 24-15 et seq. ("INCDPA"), as will be operative beginning January 1, 2026.

"UK Addendum" means the addendum to the EU Standard Contractual Clauses for the transfer of personal data to third countries compliant with the United Kingdom General Data Protection Regulation, which has Module 3 of the EU Standard Contractual Clauses incorporated and engaged by reference.

5.2 Data Processing

As a Processor, MicroStrategy will process the personal data that is uploaded or transferred to the MCE Service as instructed by Customer or provided by Customer as Controller (collectively, "Customer Data") in accordance with Customer's documented instructions. Customer authorizes MicroStrategy, on its own behalf and on behalf of the other members of its Customer Group, to process Customer Data during the term of this DPA as a Processor for the purpose set out in the table below.

Customer Data in relation to MCE Service

Subject matter of processing	Storage of data, including without limitation personal data, provided by Customer for its business purpose
Duration of processing	MCE Service Term and 90 days following expiry of such term
Nature of processing	Storage, back-up, recovery, and processing of Customer Data in connection with the MCE Service. All data is encrypted at rest.
Purpose of processing	Provision of the MCE Service
Type of personal data	The Customer Data uploaded or transferred for processing through the MCE Service by the Customer
Categories of data subject	Employees or agents of the Customer and Customer's customers, prospects, business partners and vendors, and those individuals who have been authorized to use the MCE Service by the Customer

The parties acknowledge and agree that any personal data Customer discloses to MicroStrategy in connection with this DPA is disclosed for limited business purposes and in accordance with the documented instructions for processing in connection with the performance of MCE Services pursuant to this DPA and as set forth above. The parties agree that this DPA is Customer's complete and final documented instructions to MicroStrategy in relation to Customer Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between MicroStrategy and Customer, including agreement on any additional fees payable by Customer to MicroStrategy for carrying out such instructions. Customer shall ensure that its instructions comply with all laws, rules, and regulations applicable in relation to Customer Data, and that the processing of Customer Data in accordance with Customer's instructions will not cause MicroStrategy to be in breach of Applicable Data Protection Law and/or this DPA or applicable agreements with Sub-Processors, including the EU Standard Contractual Clauses and UK Addendum. MicroStrategy will not process Customer Data outside the scope of this DPA.

MicroStrategy will:

1. Process Customer Data only on documented instructions from Customer (unless MicroStrategy or the relevant Sub-Processor (see Section 5.4 below) is required to process Customer Data to comply with applicable laws, in which case MicroStrategy will notify Customer of such legal

requirement prior to such processing unless such applicable laws prohibit notice to Customer on public interest grounds);
2. Promptly inform the Customer if, in its reasonable opinion, any instruction received from the Customer infringes Applicable Data Protection Law;
3. Ensure that any individual authorized by MicroStrategy to process Customer Data complies with Section 5.2(1) above; and
4. At the option of Customer, delete or return to Customer all Customer Data after the end of the provision of the MCE Service, relating to processing, and delete any remaining copies. MicroStrategy will be entitled to retain any Customer Data which it has to keep to comply with any applicable law or which it is required to retain for insurance, accounting, taxation, or record keeping purposes. Section 5.3 will continue to apply to retained Customer Data.

MicroStrategy will not:

1. "sell" (as defined by the CCPA) any Customer Data received or obtained in connection with performing the services specified in the Governing Agreement, or share such Customer Data for cross-contextual behavioral advertising;
2. collect, access, use, disclose, process, or retain Customer Data for any purpose other than for the specific purpose of performing the services specified in the Governing Agreement, or another business purpose permitted by Applicable Data Protection Law;
3. further collect, access, use, disclose, process, or retain Customer Data for outside of the direct business relationship between Customer and MicroStrategy; and
4. combine Customer Data received or obtained in connection with performing the services specified in the Governing Agreement with any personal data it receives from or on behalf of another person or persons, or that it collects from its own interactions, except as otherwise permitted by Applicable Data Protection Law.

MicroStrategy certifies that it understands and will comply with all restrictions in section 5.2, and that it will immediately, no later than within five (5) business days, inform Customer if it can no longer comply with obligations under Applicable Data Protection Law, including any applicable obligations under the CCPA, with respect to processing Customer Data. Upon receiving such notice, Customer may take commercially reasonable and appropriate steps to stop and remediate any unauthorized use of such Customer Data.

5.3 Confidentiality

MicroStrategy will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a government or law enforcement agency (such as a subpoena or court order). If a government or law enforcement agency sends MicroStrategy a demand for Customer Data, MicroStrategy will attempt to redirect the government or law enforcement agency to request that data directly from the Customer. As part of this effort, MicroStrategy may provide Customer's basic contact information to the government or law enforcement agency. If compelled to disclose Customer Data to a government or law enforcement agency, then MicroStrategy will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy, unless MicroStrategy is legally prohibited from doing so. MicroStrategy restricts its personnel from processing Customer Data without authorization by MicroStrategy, and imposes appropriate contractual obligations upon its personnel, including, as appropriate, relevant obligations regarding confidentiality, data protection, and data security. If the EU Standard Contractual Clauses or UK Addendum apply, nothing in this Section 5.3 varies or modifies the EU Standard Contractual Clauses or UK Addendum, including without limitation the obligations within clause 5(a).

5.4 Sub-Processing

Customer provides general authorization to MicroStrategy to engage its own affiliated companies for the purposes of providing the MCE Service and to use Sub-Processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf. The MicroStrategy website at https:// community.microstrategy.com/s/article/GDPR-Cloud-Sub-Processors list the Sub- Processors appointed by MicroStrategy that are currently engaged to carry out specific processing activities on behalf of Customer. Customer hereby consents to MicroStrategy's use of Sub-Processors as described in this Section 5.4. Before MicroStrategy engages any new Sub-Processor to carry out specific processing activities, MicroStrategy will update the applicable website. If Customer objects to a new Sub-Processor, Customer shall inform MicroStrategy in writing within thirty (30) days following the update of the applicable Sub-Processors list and such objection shall describe Customer's legitimate reasons for objection. If Customer objects to the use of a new Sub-Processor pursuant to the process provided under this Section 5.4, MicroStrategy will not engage such Sub-Processor to carry out specific processing activities on behalf of Customer without Customer's written consent. Further, MicroStrategy shall have the right to cure any objection by, in its sole discretion, either choosing to a) take any corrective steps requested by Customer in its objection (which steps will be deemed to resolve Customer's objection) and proceed to use such Sub-Processor or b) suspend and/or terminate any product or service that would involve the use of such Sub-Processor.

If MicroStrategy appoints a Sub-Processor, MicroStrategy will (i) restrict the Sub-Processor's access to Customer Data only to what is necessary to provide the MCE Service to Customer and will prohibit the Sub-Processor from accessing Customer Data for any other purpose; (ii) will enter into a written agreement with the Sub- Processor; (iii) to the extent the Sub-Processor is performing the same data processing services that are being provided by MicroStrategy under this DPA, impose on the Sub-Processor substantially similar terms to those imposed on MicroStrategy in this DPA; and (iv) comply with the EU Standard Contractual Clauses and/or UK Addendum (where applicable), which separately contain obligations in respect of the terms to be imposed in respect of an onward transfer of Personal Data to a Sub-Processor. MicroStrategy will remain responsible to the Customer for the performance of the Sub-Processor's obligations.

5.5 Transfers of Personal Data by Region

With respect to Customer Data containing personal data that is uploaded or transferred to the MCE Service, Customer may specify the geographic region(s) where that Customer Data will be processed within MicroStrategy's Sub-Processor's network (e.g., the EU-Dublin region). A Sub-Processor will not transfer that Customer Data from Customer's selected region except as necessary to maintain or provide the MCE Service, or as necessary to comply with a law or binding order of a law enforcement agency.

To provide the MCE Service, Customer acknowledges and confirms MicroStrategy may make International Transfers of Customer Data including onward transfers to its affiliated companies and/ or Sub-Processors.

MicroStrategy Incorporated and MicroStrategy Services Corporation participate in the EU-US Data Privacy Framework (DPF) and the Swiss-US DPF and have certified compliance with the principles of the DPF issued by the Department of Commerce, regarding the collection, use and retention of EU personal data transferred to the United States. Any transfers from the United States to third-party countries will be considered an "onward transfer" under the DPF. Where MicroStrategy Incorporated and MicroStrategy Services Corporation makes an onward transfer, they will ensure a contract is in place with that party which satisfies the onward transfer accountability requirements of the DPF.

MicroStrategy has also separately signed (as data exporter) with its Sub-Processors (as data importers) (a) a copy of the EU Standard Contractual Clauses and where applicable, (b) a copy of the UK

Addendum to safeguard those International Transfers which occur. In the event that the form of the EU Standard Contractual Clauses or UK Addendum is changed or replaced by the relevant authorities under Applicable Data Protection Law, MicroStrategy shall complete the updated form of the EU Standard Contractual Clauses and/or UK Addendum and notify the Customer as Controller of such form. Provided that such form is accurate and applicable to MicroStrategy as Processor, such form shall be binding on the parties (which may include the Customer and/or Sub-Processor dependent on the changed or revised document) when the relevant parties have executed the revised form, subject to the expiration of a grace period, if any, determined by the relevant Supervisory Authority. If the Customer does not enter to and execute the EU Standard Contractual Clauses or UK Addendum, where it is required to do so under Applicable Data Protection Law (either out of a failure to provide the appropriate form or because, in MicroStrategy's sole discretion, Customer is unreasonably withholding, delaying or conditioning execution of such form), MicroStrategy shall have the right to suspend and/or terminate any product or service requiring International Transfer of Customer Data upon giving the Customer thirty (30) days written notice.

For International Transfers which are subject to the Applicable Data Protection Law of Switzerland, the additional clauses below shall be added as an annex to this DPA:

1. "The term EU Member State in this DPA shall always include the EEA Member Countries and Switzerland."
2. "The data transfer is subject to the provisions of the GDPR. The provisions of the Swiss Data Protection Act are additionally applicable on a secondary basis."
3. "With regard to data transfers of personal data from Switzerland, the Federal Data Protection and Information Commissioner is the competent Supervisory Authority."
4. "Pursuant to the current Swiss Data Protection Act and until the revised Swiss Data Protection Act enters into force, the term personal data also includes the data of legal entities and not only natural persons."

Notwithstanding the foregoing, the EU Standard Contractual Clauses and/or UK Addendum or DPF (or obligations the same as those under the EU Standard Contractual Clauses or the UK Addendum or the DPF) will not apply if MicroStrategy has adopted an alternative recognized compliance standard for the lawful transfer of personal data outside the EEA, UK or Switzerland, to protect Customer Data.

In respect of other International Transfers, (outside of those covered by the EU Standard Contractual Clauses and/or the UK Addendum or the DPF) MicroStrategy will only make a transfer of Customer Data if:

1. Adequate safeguards are in place for that transfer of Customer Data in accordance with Applicable Data Protection Law, in which case Customer will execute any documents (including without limitation EU Standard Contractual Clauses, the UK Addendum, DPF or other such accepted transfer mechanism) relating to that International Transfer, which MicroStrategy or the relevant Sub-Processor reasonably requires it to execute from time to time; or
2. MicroStrategy or the relevant Sub-Processor is required to make such an International Transfer to comply with applicable laws, in which case MicroStrategy will notify Customer of such legal requirement prior to such International Transfer unless applicable laws prohibit notice to Customer on public interest grounds; or
3. Otherwise lawfully permitted to do so by Applicable Data Protection Law.

5.6 Security of Data Processing

MicroStrategy has implemented and will maintain appropriate technical and organizational measures, including, as appropriate:

1. Security of the MicroStrategy network;
2. Physical security of the facilities;
3. Measures to control access rights for MicroStrategy employees and contractors in relation to the MicroStrategy network; and
4. Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by MicroStrategy

MicroStrategy will ensure such technical and organizational measures provide the same level of privacy protection to any Customer Data as provided, and required, under Applicable Data Protection Law, including the CCPA, to the extent applicable. Customer may take commercially reasonable and appropriate steps to ensure that MicroStrategy uses Customer Data in a manner consistent with this DPA and Customer's obligations under the CCPA.

Customer may also elect to implement appropriate technical and organizational measures in relation to Customer Data, directly from MicroStrategy's Sub- Processor. Such appropriate technical and organizational measures include:

1. Pseudonymization and encryption to ensure an appropriate level of security;
2. Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services provided by Customer to third parties;
3. Measures to allow Customer to backup and archive appropriately to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and
4. Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

5.7 Security Breach Notification

MicroStrategy will, to the extent permitted by law, notify Customer without undue delay after becoming aware of any actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Data by MicroStrategy or MicroStrategy's Sub-Processor(s) (a "Security Incident"). To the extent such a Security Incident is caused by a violation of the requirements of this DPA by MicroStrategy, MicroStrategy will make reasonable efforts to identify and remediate the cause of such a breach, including steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Customer agrees that an unsuccessful Security Incident will not be subject to this Section 5.7. An unsuccessful Security Incident is one that results in no actual unauthorized access to Customer Data or to any of MicroStrategy's or MicroStrategy's Sub-Processor's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-in attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents; and MicroStrategy's obligation to report or respond to a Security Incident under this Section 5.7 is not, and will not, be construed as an acknowledgment by MicroStrategy of any fault or liability of MicroStrategy with respect to the Security Incident.

Notification(s) of Security Incidents, if any, will be delivered to Customer by any means MicroStrategy selects, including via email. It is Customer's responsibility to ensure that they provide MicroStrategy with accurate contact information and secure transmission at all times.

The information made available by MicroStrategy is intended to assist Customer in complying with their obligations under Applicable Data Protection Law in respect of data protection impact assessments and prior consultation.

5.8 Audit

MicroStrategy will allow for and contribute to audits (including those under the EU Standard Contractual Clauses/UK Addendum where these apply), which shall include inspections, conducted by Customer or another auditor mandated by Customer, provided that the Customer gives MicroStrategy at least 30 days' reasonable prior written notice of such audit and that each audit is carried out at Customer's cost, during business hours, at MicroStrategy nominated facilities, and so as to cause the minimum disruption to MicroStrategy's business and without Customer or its auditor having any access to any data belonging to a person other than Customer. Any materials disclosed during such audits and the results of and/or outputs from such audits will be kept confidential by Customer. Such audit shall be performed not more than once every 12 months, and Customer shall not copy or remove any materials from the premises where the audit is performed.

Customer acknowledges and agrees (having regard to Section 5.4(iii)) that in respect of MicroStrategy's auditing rights of its Sub-Processor providing infrastructure services for the MCE Service, such Sub-Processor will use external auditors to verify the adequacy of security measures including the security of the physical data centers from which the Sub-Processor provides the Services. This audit will be performed at least annually according to ISO 27001 standards or other such alternative standards that are substantially equivalent to ISO 27001 by independent third-party security professionals at the Sub-Processor's selection and expense, and will result in the generation of an audit report ("Report"), which will be the Sub-Processor's confidential information or otherwise be made available subject to a mutually agreed upon non-disclosure agreement covering the Report ("NDA"). MicroStrategy will not be able to disclose such Report to Customer without permission from the Sub-Processor. At Customer's written request during the exercise of its audit rights under this Section 5.8, MicroStrategy will request the permission of the Sub-Processor to provide Customer with a copy of the Report so that Customer can reasonably verify the Sub-Processor's compliance with its security obligations. The Report will constitute confidential information and the Sub-Processor may require Customer to enter into an NDA with them before releasing the same.

If the EU Standard Contractual Clauses or UK Addendum apply under Section 5.5, then Customer agrees to exercise its audit and inspection right by instructing MicroStrategy to conduct an audit as described in this Section 5.8, and the parties agree that notwithstanding the foregoing, nothing varies or modifies the EU Standard Contractual Clauses or UK Addendum nor affects any Supervisory Authority's or Data Subject's rights under those EU Standard Contractual Clauses or UK Addendum.

5.9 Independent Determination

Customer is responsible for reviewing the information made available by MicroStrategy and its Sub-Processor relating to data security and making an independent determination as to whether the MCE Service meets Customer's requirements and legal obligations as well as Customer's obligations under this DPA.

5.10 Data Subject Rights

Taking into account the nature of the MCE Service, Customer can utilize certain controls, including security features and functionalities, to retrieve, correct, delete, or restrict Customer Data. MicroStrategy will provide reasonable assistance to Customer (at Customer's cost) in:

1. Complying with its obligations under the Applicable Data Protection Law relating to the security of processing Customer Data;

2. Responding to requests for exercising Data Subjects' rights under the Applicable Data Protection Law, including without limitation by appropriate technical and organizational measures, insofar as this is possible;
3. Documenting any Security Incidents and reporting any Security Incidents to any Supervisory Authority and/or Data Subjects;
4. Conducting privacy impact assessments of any processing operations and consulting with supervisory authorities, Data Subjects, and their representatives accordingly; and
5. Making available to Customer information necessary to demonstrate compliance with the obligations set out in this DPA.

5.11 Return or Deletion of Customer Data

Due to the nature of the MCE Service, MicroStrategy's Sub-Processor provides Customer with controls that Customer may use to retrieve Customer Data in the format in which it was stored as part of the MCE Service or delete Customer Data. Up to the termination of the Governing Agreement between Customer and MicroStrategy, Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this Section 5.11. For 90 days following that date, Customer may retrieve or delete any remaining Customer Data from the MCE Service, subject to the terms and conditions set out in the Governing Agreement, unless (i) it is prohibited by law or the order of a governmental or regulatory body, (ii) it could subject MicroStrategy or its Sub-Processors to liability, or (iii) Customer has not paid all amounts due under the Governing Agreement. No later than the end of this 90-day period, Customer will close all MicroStrategy accounts. MicroStrategy will delete Customer Data when requested by Customer through the MCE Service controls provided for this purpose.

Appendix A - Cloud Support Offerings

	Cloud Support	Cloud Elite Support
Issue resolution by dedicated Cloud Technical Account Manager	Yes	Yes
Number of designated Support Liaisons	4	8
Architect Education Passes	0	8
Initial response times for P1 and P2 issues* ***priority definitions as provided in the Technical Support Policy and Procedures**	P1 < 2hr P2 < 2hr	P1 < 15 minutes P2 < 1 hour
P1 and P2 issues updates	As status changes or daily	P1 every 1 hour P2 as status changes or twice a day
Case management meetings	No	Weekly
System alert notifications	No	Customizable
Quarterly service reporting	Via email	Via meeting
Location based 24x7 support	No	Yes

Appendix B - RACI Diagram

ACTIVITY	DESCRIPTION	MCE STANDARD	CUSTOMER
Cloud Platform			
Environment Build	Automated build, security boundaries, etc.	RA	CI
Infrastructure Maintenance	Monthly/Emergency Maintenance Windows, OS Updates	RA	I
Environment Resizing	Upsizing/Downsizing of the VMs	RA	CI
Infrastructure Management	All cloud components such as VMs, Storage, DBMS (for MD/PA)	RA	
Backups	Compute Instances, cache/cubes files, MD Repository, ODBC and Config files	RA	
Restores	Compute Instances, cache/cubes files, MD Repository, ODBC and Config files	RA	CI
24x7 Support		RA	
Security & Compliance			
ISO27001	Certifications with 3rd party audit	RA	I
SOC2/Type 2	Certifications with 3rd party audit	RA	I
GDPR	Certifications with internal audit	RA	I
PCI	Certifications with internal audit	RA	I
HIPAA	Certifications with 3rd party audit	RA	I
24x7 Security Incident Event Management	Security logs sent to SIEM for automatic analyses	RA	I
Vulnerability Management	Scanning, remediation following the NIST standards	RA	I
Penetration Testing	Quarterly environmental external scanning	RA	I
Data Encryption at Rest	AES 256 encryption on storage volumes and MD DB	RA	I
Monitoring			
Cloud Infrastructure Components	VMs, Storage, DBMS (for MD/PA), Network components	RA	I
Application Services	MicroStrategy Components like I-Server, WebApps, etc.	RA	I
Data Connectivity	VPN, PrivateLink	RA	CI
Intrusion Detection	SIEM	RA	I
Networking Connections	On-Premise Connectivity for internal access	RA	CI
Networking			

Logging	Load balancer logs, etc.	RA	
Data source and Databases connections	Deployment/configuration of VPN Tunnels, Private Links, Express route, etc.	RA	RA
Networking Connections	On-Premise Connectivity for internal access	RA	RA
MicroStrategy Application Administration			
Reference Architecture	MicroStrategy Cloud Environment Architecture	RA	I
Upgrades	Platform Upgrades via parallel environments	R	ACI
Description	Over the top Updates - no parallel environment required	R	ACI
Post Upgrade QA (Availability of the Services)	Testing and Validation of Services health/availability	RA	CI
Post Upgrade Regression Testing	Customer Regression and functional tests/certifications	I	RA
Customer Data	Customer Data		RA
MicroStrategy Project Development	Content building and delivery		RA
MicroStrategy Project and I-Server Configuration	Project and I-Server specific settings		RA
Customizations	Custom workflows, plugins/SDK Customizations, MicroStrategy Webapps Customizations	CI	RA
MicroStrategy Application User Permissions	Customer controls who has access to what reports		RA
Authentication set up	SSO and OIDC Supported Authentication Methods	R	ACI
Metadata Modelling	Building rules		RA
Platform Analytics	Initial configuration only + Monitoring of availability of the services	RA	
SMTP Server for Distribution Services	Your MCE's DS sent via your own SMTP server	CI	RA
File Subscriptions	Customer configures to send content to files on disk (Blob or S3 or Google Cloud Storage)	RA	CI
Plugins		CI	RA
Pre-Prods/POC			

Project Management	Aligning internal resources to complete activities. Highlighting areas of customer responsibility (SE led)	RA	CI
Build Environment (Vanilla)	Based on the platform and region of choice	RA	CI
MicroStrategy MD Restore	Restore MD and other artifacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Networking Connections	On-Premise Connectivity for internal access	RAC	ACI
Customizations	Custom workflows, plugins/SDK Customizations, MicroStrategy Webapps Customizations	CI	RAC
Testing	Testing to ensure success criteria is met (SE led with customer)	CI	RA
Migrations			
Project Management	Aligning internal resources to complete activities. Highlighting areas of customer responsibility	R	ACI
Application Upgrade	Upgrade of MD and other artifacts to the latest version	RA	CI
MicroStrategy MD Restore/Refresh	Restore/Refresh MD and other artifacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Networking Connections	On-Premise Connectivity for internal access	RAC	ACI
Customizations	Custom workflows, plugins/SDK Customizations, MicroStrategy Webapps Customizations	CI	RAC
Post Upgrade QA (Availability of the Services)	Testing and Validation of Services health/availability	RA	CI
Post Upgrade Regression Testing	Customer Regression and functional tests/certifications	CI	RA

MicroStrategy Incorporated, 1850 Towers Crescent Plaza, Tysons Corner, VA 22182

microstrategy.com