Strategy

Managed Cloud Standard

Service Guide

Update Published: April 2026

Copyright Information

Trademark Information

The following are either trademarks or registered trademarks of Strategy 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, Strategy, Strategy 2019, Strategy 2020, Strategy 2021, Strategy Analyst Pass, Strategy Architect, Strategy Architect Pass, Strategy Auto, Strategy Cloud, Strategy Cloud Intelligence, Strategy Command Manager, Strategy Communicator, Strategy Consulting, Strategy Desktop, Strategy Developer, Strategy Distribution Services, Strategy Education, Strategy Embedded Intelligence, Strategy Enterprise Manager, Strategy Federated Analytics, Strategy Geospatial Services, Strategy Identity, Strategy Identity Manager, Strategy Identity Server, Strategy Insights, Strategy Integrity Manager, Strategy Intelligence Server, Strategy Library, Strategy Mobile, Strategy Narrowcast Server, Strategy ONE, Strategy Object Manager, Strategy Office, Strategy OLAP Services, Strategy Parallel Relational In-Memory Engine (Strategy PRIME), Strategy R Integration, Strategy Report Services, Strategy SDK, Strategy System Manager, Strategy Transaction Services, Strategy Usher, Strategy Web, Strategy Workstation, Strategy World, Usher, and Zero-Click
Intelligence.

The following design marks are either trademarks or registered trademarks of Strategy 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. Strategy is not responsible for errors or omissions. Strategy makes no warranties or commitments concerning the availability of future products or versions that may be planned or under development.

Table of Contents

Overview

The Managed Cloud Standard service ("MCS" or "MCS Service") is a Software-as-a-service ("SaaS") offering that Strategy manages on its customers' behalf in an Amazon Web Services environment that includes access to, collectively, (a) the "Cloud Platform" version of Strategy software products (an optimized version of the Strategy One software platform built specifically for deployment in an Amazon Web Services environment) licensed by the customer; and (b) Cloud Support, as described below.

Cloud Support

As a Managed Cloud Standard service customer, you will receive "Cloud Application Support" ("Cloud Support") in which our Cloud Support team will provide ongoing monitoring, upgrades and maintenance over your MCS Service term. Cloud Support includes a default environment configuration. If an outage occurs, Strategy reserves the right to fix the issue on behalf of the customer without pre-authorization. See Appendix A for more detail.

Cloud Infrastructure

Our MCS Service offers a dedicated Strategy environment built based on industry best practices for security, compliance, and availability. Strategy's MCS Architecture consists of a single container-based environment composed of the core Strategy One components including Intelligence Server, Library, and Collaboration services. There is also a database to support Strategy metadata and collaboration services. The Cloud Architecture for MCS includes the following components:

- Sold on a per user pricing model, starting at 50 Standard User licenses and 2 Standard Architect licenses.
- MCS has the ability to scale up to 300 Standard User licenses and 2 Standard Architect licenses.
- All user licenses are provided with 0.5GB of allocated memory with a minimum of 25 GB memory allocated.
- MCS Environments, based on licenses, can scale to support a maximum of 150 GB total memory.

Strategy will provide Cloud Environment Support through an MCS Service subscription, ensuring your environments are maintained effectively. MCS environments will be monitored and kept available 24/7, subject to any applicable exclusions of availability including but not limited to:

1. **Scheduled Maintenance**: Service interruptions during scheduled maintenance, announced in advance, are excluded from the SLA.

2. **Customer Configurations**: Service issues caused by customer actions, such as misconfigurations or excessive API requests, are not covered. Issues related to applications built on the Strategy software platform, including project, report,

and document issues; migration problems related to user design; downtime experienced as a result of user activity.

3. **ETL Application:** Outages caused through degradation or failure of ETL processes in the application.
4. **Database Issues and Configuration:** Improper database logical design and code issues.
5. **HyperScaler or other Third-party Services**: Downtime related to third-party services or dependencies outside control is excluded.
6. **Force Majeure**: Events beyond control of Strategy, such as natural disasters or government actions, do not qualify for SLA coverage.
7. **Unauthorized Access**: Issues not originated by Strategy like unauthorized access or credential compromised
8. **Customer-Based Migration Issues:** Migration problems and outages related to customer or user design.
9. **SSO or other Custom Security Configuration or Policies**: Implementation and management of custom security policies and compliance measures outside the pre-configured, standard security settings are not included.
10. **Network Connectivity Issues**: Issues related to the customer's internal network or internet connectivity, including VPN configurations and local firewall settings, fall under the customer's responsibility.

Backups

Daily backups are performed for all customer systems, including system state and metadata. By default, MCS customers will have a seven (7) day backup retention period only. All backups are inclusive of metadata, data storage services, cubes, and caches.

Maintenance

Maintenance windows are scheduled monthly to allow for third-party security updates to be applied to the MCS platform. During these scheduled interruptions, the MCS 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, Maintenance windows will be defined as part of set monthly schedule upon purchase Emergency maintenance work is required, we will use commercially reasonable efforts to give 24-to-48-hour notice before applying a remedy. MCS customers are required to adhere to their monthly maintenance window.

Updates and Upgrades

Strategy is committed to providing the latest updates with security fixes, therefore all customers are required to take advantage of the fixes and new features. Strategy will Update or Upgrade your environment every month, at no charge, including any security fixes as well as new features delivered across the Strategy One platform.

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 Strategy One 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 MCS 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 MCS 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 MCS Service Order Form. You may not perform any penetration testing on the artificial intelligence service powering the AI Capabilities.

Security

Various security tools are employed to perform penetration testing and remediation, system event logging, and vulnerability management. The MCS 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 MCS 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. MCS 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.

MCS Security Scans

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

Cloud Shared Services Components

As part of the MCS 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.

Terms Applicable to Processing Personal Data

This section will apply only to the extent there is no other executed agreement in place regarding the same subject between Strategy and the customer ("Customer"), including any Order Form(s) and/or a master agreement between the customer and Strategy (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.

Definitions

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

"Data Privacy Framework" means, as relevant, (i) the EU-US Data Privacy Framework as administered by the US Department of Commerce and approved by the European Commission as ensuring an adequate level of protection for Personal Data for the purposes of Article 45 GDPR; (ii) the UK Extension to the EU-US Data Privacy Framework approved by the competent authority of the United Kingdom as ensuring an adequate level of protection for Personal Data for the purposes of Article 45 UK GDPR; and (iii) the Swiss-US Data Privacy Framework as administered by the US Department of Commerce and approved by the Swiss Federal Administration as ensuring an adequate level of protection for Personal Data for the purposes of applicable Swiss data protection laws, in each case as in force, amended, consolidated, re-enacted or replaced from time to time.

"**EU/UK Privacy Laws**" means, as applicable: (a) the General Data Protection Regulation 2016/679 (the "**GDPR**"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018, the UK General Data Protection Regulation as defined by the UK Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (together with the UK Data Protection Act 2018, the "**UK GDPR**"), and the Privacy and Electronic Communications Regulations 2003; and (d) any relevant law, directive, order, rule, regulation or other binding instrument which implements any of the above, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

"**Personal Data**" means any information Strategy processes on behalf of Customer to provide the Services that is defined as "personal data" or "personal information" under any Privacy Law. "**Privacy Laws**" means, as applicable, EU/UK Privacy Laws, US Privacy Laws and any similar law of any other jurisdiction which relates to data protection, privacy or the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.
"**Security Incident**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Personal Data. For the avoidance of doubt, an unsuccessful attempt that does not result in the unauthorized access to Personal Data or to any of Strategy's or
Strategy's sub-processor's equipment or facilities storing Personal Data including, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful logon 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 shall not be considered a Security Incident.
"Sub-Processor" means any third party appointed by Strategy to process personal data.
"**Third Country**" means any country or territory outside of the scope of the data protection laws of the European Economic Area or the UK, as relevant; that has not been approved as providing adequate protection for Personal Data by the relevant competent authority from time to time.
"**US Privacy Laws**" means, as applicable, the California Consumer Privacy Act, Colorado Privacy Act, Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, Florida Digital Bill of Rights,
Indiana Consumer Data Protection Act, Iowa Consumer Data Protection Act, Montana Consumer Data Privacy Act, Oregon Consumer Privacy Act, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, and Virginia Consumer Data Protection Act, and any similar law of any other state related to the processing of Personal Data.

Data Processing

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

Personal Data in relation to MCS Service

Subject matter of processing	Storage of data, including without limitation Personal Data, provided by Customer for its business purpose
Duration of processing	MCS Service Term and 90 days following expiry of such term
Nature of processing	Storage, back-up, recovery, and processing of Personal Data in connection with the MCS Service.
Purpose of processing	Provision of the MCS Service
Type of personal data	The Personal Data uploaded or transferred for processing through the MCS 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 MCS Service by the Customer

Strategy may aggregate and/or anonymize Personal Data such that it no longer constitutes Personal Data under Privacy Laws and process such data for its own purposes. To the extent Strategy receives de-identified data (as such term is defined under applicable US Privacy Laws) from Customer, Strategy shall: (i) take commercially reasonable measures to ensure that the data cannot be associated with an identified or identifiable individual; (ii) publicly commit to maintain and use the data only in a de-identified form and not attempt to re-identify the data; and (iii) otherwise comply with applicable US Privacy Laws with respect to such de-identified data. Customer will take all measures possible to avoid transferring or providing us any access to any Personal Data to the extent possible while continuing using the MCS Service.
In processing Personal Data under the Agreement, Strategy will:

1. only process Personal Data on documented instructions from Customer which the Parties agree that this DPA is Customer's complete and final documented instruction to Strategy in relation to Personal Data (which the parties agree are reflected in full in this DPA), for the limited and specific purpose described in the table above, and at all times in compliance with Privacy Laws, unless required to process such Personal Data by applicable law to which Strategy is subject; in such a case, Strategy shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. notify Customer without undue delay if it: (i) makes a determination that it can no longer meet its obligations under applicable US Privacy Laws or (ii) believes that instruction of Customer, infringes applicable Privacy Laws;
3. to the extent required by Privacy Laws, and upon reasonable written notice that Customer reasonably believes Strategy is using Personal Data in violation of Privacy Laws or this DPA, grant Customer the right to take reasonable and appropriate steps to help ensure that Strategy uses the Personal Data in a manner consistent with Customer's obligations under Privacy Laws, and stop and remediate any unauthorized use of the Personal Data; and
4. require that each employee or other person processing Personal Data is subject to an appropriate duty of confidentiality with respect to such Personal Data.
5. To the extent required by applicable Privacy Laws, Strategy will not:

1. sell the Personal Data or sharing the Personal Data for cross-context behavioral advertising purposes;
2. retain, use, or disclose the Personal Data outside of the direct business relationship between Strategy and Customer and for any purpose other than for the specific purpose of performing the Services; and
3. combine the Personal Data received from, or on behalf of, Customer with any Personal Data that may be collected from Strategy's separate interactions

with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Privacy Laws.

Customer Obligations

Customer shall comply with all Privacy Laws in providing Personal Data to Strategy in connection with the Services. Customer represents and warrants that: (a) the Privacy Laws applicable to Customer do not prevent Strategy from fulfilling the instructions received from Customer and performing Strategy's obligations under this DPA; (b) all Personal Data was collected and at all times processed and maintained by or on behalf of Customer in compliance with all Privacy Laws, including with respect to any obligations to provide notice to and/or obtain consent from individuals; and (c) Customer has a lawful basis for disclosing the Personal Data to Strategy and enabling Strategy to process the Personal Data as set out in this DPA. Customer shall notify Strategy without undue delay if Customer makes a determination that the processing of Personal Data under the Agreement does not or will not comply with Privacy Laws, in which case, Strategy shall not be required to continue processing such Personal Data.

5.4 Sub-Processing

To the extent Strategy engages any Sub-Processors to process Personal Data on its behalf:

a. Customer hereby grants Strategy general written authorization to engage the Sub-

Processors set out on the Strategy's website, currently at: https://community.Strategy.com/s/article/GDPR-Cloud-Sub-Processors, (as such website addresses may be amended or replaced from time to time), subject to the requirements of this section.

b. If Strategy appoints a new Sub-Processor or intends to make any changes concerning the addition or replacement of any Sub-Processor which will process Personal Data that Strategy is processing on behalf of Customer, Strategy shall update the websites set out in Section 5.4(a) above and inform Customer of such update via e-mail if the new or replacement Sub-Processor will process any Personal Data. If Customer fails to object to the appointment or replacement within thirty (30) days' of its posting on reasonable and documented grounds related to the confidentiality or security of Personal Data or the subcontractor's compliance with Privacy Laws, Strategy may proceed with the appointment or replacement. If Customer reasonably objects to a new sub-processor, Customer shall inform Strategy in writing within thirty (30) days following the update of the applicable Sub-Processor list and such objection shall describe Customer's legitimate reasons for objection. Strategy shall have the right to cure any objection by, in its sole discretion, either choosing to (i) take any corrective steps requested by Customer in its objection (which steps will be deemed to resolve Customer's objection) and proceed to use the Sub-Processor or (ii) suspend and/or terminate any product or service that would involve the use of the sub-processor.

c. Strategy shall engage Sub-Processors only pursuant to a written agreement that contains obligations on the subcontractor which are no less onerous on the relevant subcontractor than the obligations on Strategy under this DPA.
d. In the event Strategy engages a Sub-Processor to carry out specific processing activities on behalf of Customer pursuant to EU/UK Privacy Laws, where that SubProcessor fails to fulfil its obligations, Strategy shall remain fully liable under applicable EU/UK Privacy Laws to Customer for the performance of that Sub-Processor's obligations.

Transfers of Personal Data

Customer acknowledges and agrees that Strategy may appoint an affiliate or third-party subprocessor to process the Personal Data in a Third Country, in which case, Strategy shall ensure that any Personal Data transferred to such affiliate or third-party shall be done so pursuant to a valid data transfer mechanism under EU/UK Privacy Laws, such as the Data Privacy Framework (if applicable) or the standard contractual clauses for the transfer of Personal Data to third countries.

Security of Data Processing

Strategy shall, taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purpose of the processing, implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risk.
Customer may also elect to implement appropriate technical and organizational measures in relation to Customer Personal Data, directly from Strategy'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 Personal 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.

Security Breach Notification

To the extent required by Privacy Laws, Strategy shall without undue delay notify Customer of any Security Incident, with further information about the Security Incident provided in phases as more details become available. For the avoidance of doubt, Strategy's obligation to report or respond to a Security Incident, including without

limitation, under this section is not and will not be construed as an acknowledgement by Strategy of any fault or liability of Strategy with respect to the Security Incident.

Audit

Upon reasonable request of Customer, Strategy shall make available to Customer such information in its possession as is reasonably necessary to demonstrate Strategy's compliance with its obligations under this DPA, and allow for and contribute to audits by providing written responses to questionnaires and copies of relevant documents. As an alternative to an audit performed by the Customer, to the extent permitted by Privacy Laws, Strategy may arrange for a qualified and independent auditor to conduct, at Customer's expense, an assessment of Strategy's policies and technical and organizational measures in support of its obligations under Privacy Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessment, and will provide a report of such assessment to Customer upon reasonable request. Notwithstanding the foregoing, in no event shall Strategy be required to give Customer access to information, facilities, documents or systems to the extent doing so would cause Strategy to be in violation of confidentiality obligations owed to other customers or its legal obligations.

Customer acknowledges and agrees that our rights to audit our Sub-Processors referred to in the Transfers of Personal Data section above will be subject to the terms we have in place with each such Sub-Processor and will likely involve: (i) using 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; (ii) ISO 27001 standards or other such alternative standards that are substantially equivalent to ISO 27001; and (iii) 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**"). Strategy may not be able to disclose such Report to Customer without permission from the Sub-Processor. At Customer's reasonable written request during the exercise of its audit rights under the Independent Determination section below, Strategy will request the permission to provide Customer with a copy of such Report so that Customer can reasonably verify the Sub-Processor's compliance with its security obligations, provided that Customer acknowledges that the Sub-Processor may require Customer to enter into an NDA with such Sub-Processor before releasing the same.

Independent Determination

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

Assistance

To the extent required by Privacy Laws, and taking into account the nature of the processing, Strategy shall, in relation to the processing of Personal Data and to enable Customer to comply with its obligations which arise as a result thereof, provide

reasonable assistance to Customer, through appropriate technical and organizational measures, in:

a. responding to requests from individuals pursuant to their rights under Privacy Laws, including by providing, deleting or correcting the relevant Personal Data, or by enabling Customer to do the same, insofar as this is possible;
b. implementing reasonable security procedures and practices appropriate to the nature of the Personal Data to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure;
c. notifying relevant competent authorities and/or affected individuals of any Security Incident;
d. conducting data protection impact assessments and, if required, prior consultation with relevant competent authorities; and
e. entering into this DPA.

Return or Deletion of Customer Data

Due to the nature of the MCS Service, Strategy'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 MCS Service or delete Customer Data. Up to the termination of the Governing Agreement between Customer and Strategy, Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this section For 90 days following that date, Customer may retrieve or delete any remaining Customer Data from the MCS 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 Strategy 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 Strategy accounts. Strategy will delete Customer Data when requested by Customer through the MCS Service controls provided for this purpose.

Appendix A - Cloud Support Offerings

Support Detail	Cloud Support
Designated Customer Success Manager (CSM)	No
Number of designated Support Liaisons	2
Initial response times for P1 and P2 issues* *priority definitions as provided in the Technical Support Policy and Procedures	P1 < 2hr P2 < 2hr
P1 and P2 issues updates	As status changes
Case management meetings	No
System alert notifications	No
Location based 24x7 support	No

Strategy

1850 Towers Crescent Plaza | Tysons Corner, VA 22182 |
strategysoftware.com