Veritas Alta^{TM} SaaS Protection

December 2023 Service Description

Service Overview

The Veritas Alta SaaS Protection service ("Service") consists of cloud-native software running in Microsoft Azure datacenters as a Software-as-a-Service (SaaS) offering. The Service is provided through a combination of installable software components and the Tenant to enable backup, recovery, eDiscovery, archiving, analytics, and tiering of data with the Customer's target applications and infrastructure.

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for those Services which are described in this Service Description and are provided by Veritas.

Service Offerings

Service Features

Veritas provides the following package options based on customer backup and data management needs. A customer must purchase the same package option across all their licenses.

	Enterprise	Enterprise Plus
Data Protection		
Data source connectors[1] Customer can protect its workloads through secured connections by use of data source connectors. More details in the Connector Types section.	●	●
Custom backup policies Customer can set backup scope and schedules according to its needs.	●	●
Automated backups Users enroll into scheduled backups that occur automatically.	●	●
Restore levels Customer can perform fine-grained and bulk recoveries according to its needs.	●	●
Restore options Backups can be recovered in-place, to a new or alternate location, across Microsoft 365 tenants, or to external destination.	●	●
Reporting and analytics The Service portal provides customer with the ability to monitor and report backup status and coverage.	●	●
Data Governance		
Legal hold Customer data can be preserved for litigation.	●	●

eDiscovery early case management Customers can create and manage cases for litigation and data privacy needs.	●	●
Metadata search Customers can search by usernames, files, folders, dates.	●	●
Full-text search Customers can search content within files.	Not available	●
Security		
Data encryption in-flight and at-rest Customer Data is encrypted using AES-256-bit encryption.	●	●
Azure AD integration Services have integrated support for MFA and SSO.	●	●
IP allowed/restricted list Customers can setup allowed or restricted IP lists.	●	●
Audit log Customers can query and report on the activity histories of users and system processes.	●	●
Compliance		
Custom retention policies Customers can apply immutable retention periods, subject to maintaining an active Service subscription.	●	●
Data residency Customers can select the Azure hosting region(s) for Customer Data.	●	●
Local redundancy (3 copies) Backups are synchronous replicated for high availability.	●	●
Geo-scale out, multi-region Customers can manage data sovereignty centrally for users from multiple geographies (requires pricing and deployment for each additional region).	Not available	●
Administration		
Role-based access control Customers can setup and control access of various types of users.	●	●
End user self-service access Customers can enable end users to browse, search, share, and retrieve their data on their own.	Not available	●
Add-On Services (subject to additional fees)		
Extra Data Backup Customers can make an additional backup of their air-gapped data to another location (three copies of the data). Unless a Customer has purchased Extra Data Backup for Azure blob under a Veritas-Hosted Tenant, Customers must have a separate cloud subscription (Azure, AWS, etc.) to provide a location for the extra data backup and is responsible for any of its cloud hosting costs associated with this backup.	●	●

Additional Storage Customers can increase the data storage capacity of their Tenant.	●	●
Software Development Kit (SDK) Customers interested in creating their own custom connectors or in integrating Veritas Alta SaaS Protection into one of their own applications can obtain an SDK.	●	●

[1] Data source connector type(s) depends on license purchased (i.e., Exchange Online, Box, Slack, etc.)

Connector Types

Microsoft 365 Suite	• Provides backup and recovery for Exchange Online, OneDrive, SharePoint Online and Teams, as well as O365 Audit logs. • License meter is per user. • Users will count once across Exchange Online, OneDrive, SharePoint Online and Teams. • A user license includes a storage allocation of 20 GB per user.
Microsoft 365 Exchange Online	• Provides backup and recovery for mailbox items that include Email, calendar, contacts, tasks, and notes. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Microsoft 365 OneDrive	• Provides backup and recovery for OneDrive items that include files, folders and permissions. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Microsoft 365 SharePoint Online	• Provides backup and recovery for SharePoint items that include all list items from any content type within site collections, including permissions and all item metadata. License meter is per user. • A user license includes a storage allocation of 10 GB per user.

Microsoft 365 Teams	• Provides backup and recovery for Teams items that include Team sites, members, member permissions, channels, posts, files and wiki. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Salesforce	• Provides backup and recovery for structured data elements (including standard and custom objects and records). • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Box	• Provides backup and recovery for Box items that include files, folders and permissions. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Slack	• Slack provides backup and recovery for Slack items that include workspaces, channels, messages, and files. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Google Workspace	• Provides backup and recovery for Google Mail and Google Drive items that include files, folders, and permissions. • License meter is per user. • A user license includes a storage allocation of 20 GB per user.

Entra ID (formerly Azure AD)	• Provides backup and recovery of users, groups, app registrations and enterprise applications • Ability to auto-restore relationships (with limitations) and restore deleted objects (within last 30 days) • License meter is per user • A user license includes a storage allocation of 200 MB per user.
Structured Data	• Provides backup, recovery, and archiving for small file-size workloads that are generally high in object count, thus requiring higher performance compute and storage compared to Unstructured Data workloads. • License meter is per FETB.
Unstructured Data – Cool	• Provides backup, recovery, tiering and archiving for Unstructured Data that requires immediate retrieval/access whenever necessary. • The following workloads are supported: ○ File systems: Microsoft Windows Server, Linux, UNIX ○ Object storages: Azure Blob, Azure Files, AWS S3 • License meter is per FETB.
Unstructured Data – Archive	• Provides backup and long-term archiving for Unstructured Data requires cost-efficient storage but does not need immediate retrieval response times. • The following workloads are supported: ○ File systems: Microsoft Windows Server, Linux, UNIX ○ Object storages: Azure Blob, Azure Files, AWS S3 • License meter is per FETB.

Veritas reserves the right to move Customer Data under a Per User Connector Type that has not been accessed by Customer for a year or longer to an archive tier within Azure. Any backups of Customer Data from an archive tier can still be restored but will take additional time to do so.

Service Components

Some Connector Types may require use of a Software Component. Customer's right to use such Software Component begins when the Service is activated and ends when Customer's right to use the associated Service terminates or expires. Customer must uninstall a Software Component when Customer's right to use the associated Service terminates or expires. Veritas may disable the Software Component at that time.

Shared Storage Allocation

The storage allocation for each Connector Type is aggregated within a Tenant across all Users as determined by multiplying the quantity of Users for such Connector Type by the allocation per User, plus any FETB storage purchased under FETB-metered Connector Types. The per Connector Type storage allocation is then added to the Customer's overall shared storage capacity and enforced at the Tenant level. Customers can purchase Additional Storage to increase the overall aggregate amount of storage capacity of their Tenant.

License Enforcement

The Service alerts customers when their subscription term is about to expire. Once a subscription expires, new backups will suspend and not resume until the subscription is renewed. Otherwise, Customer Data will be decommissioned in accordance with the Data Decommissioning section.

Service Subscriptions are metered on either a per User or per FETB basis, as described in the Connector Types section above. If there are multiple connectors that are set up, usage is aggregated at the Tenant level to get the total capacity used by the connectors configured.

- For connectors with user-based licenses, the Service will alert the customer when 100% of available licenses and/or storage are used. The service will not allow more users to be added to the connector's scope once a connector has used all available licenses. New backups will be suspended and will not run until Customer either reduces capacity usage or purchases more storage.

- For connectors with user-based licenses there are limits on capacity allocated. The service will alert the customer when the data protected by the Service for a particular license type has reached 80% capacity, 90% capacity and 100% capacity or exceeds available capacity, as compared against the Shared Storage Allocation. The Service will not allow more users to be added to the connector's scope, and new backups will be suspended and will not be run until Customer either reduces capacity usage or purchases more storage.

- For connectors with front-end terabyte-based licenses, the Service will alert the customer when data protected by the Service for a particular license type has reached 80% capacity, 90% capacity, and when at 100% capacity or exceeds available capacity. Once the 100% or exceeds capacity alert is triggered, new backups will be suspended and will not be run until Customer either reduces capacity usage or purchases more licenses.

- Licenses are time-bound according to Customer's Service Subscription start and end dates. If Customer's Subscription expires, Customer will no longer have access to login to the Tenant and new backups will be suspended, and all Customer Data will be decommissioned in accordance with the Data Decommissioning section, including data with immutable retention periods or on legal hold.

Software Development Kit (SDK)

The Software Component SDK allows Customer to integrate the Service with Customer's existing systems, other Veritas products, or third-party products, subject to the limitations set forth below:

- Customer may use a reasonable number of copies of such Development Tool(s) solely in support of Customer's use of the Service for the following purposes: 1) integration with internal systems to streamline and automate processes for reporting and workflows or 2) development of software that imports or retrieves data from a third-party technology into the Service solely in support of Customer's use of the Service. Customer has no right to modify or alter the SDK and may not distribute the SDK, alone or as integrated with any other code or product, in any manner whatsoever to any third party. Customer may not use the SDK except as expressly provided herein.

- An annual subscription to the SDK is limited to ten (10) hours of engineering time. If Customer needs further support with respect to the SDK, Customer will need to purchase additional assistance from Veritas.

- Open-Source Code. Customer's license rights to the SDK are conditioned upon Customer not creating derivative works of the SDK in any manner that would cause the SDK in whole or in part to become Open-Source Code.

- Warranty Disclaimer. THE SDK IS PROVIDED "AS IS," EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ANY OTHER WARRANTY, WHETHER EXPRESSED OR IMPLIED. FURTHERMORE, VERITAS SHALL NOT BE LIABLE UNDER ANY THEORY FOR ANY DAMAGES SUFFERED BY CUSTOMER OR ANY USER OF THE SDK OR ANY APPLICATIONS PROVIDED BY CUSTOMER WHICH WERE DEVELOPED USING THE SDK.

- Development Disclaimer: Veritas shall not be responsible for any such integration, or any development and programming activities undertaken by Customer, including but not limited to use of the SDK for anything other than its intended purpose. Unless Customer uses an appropriate degree of skill and care in Customer's development and programming activities, any integration may cause errors or problems in the use or operation of the Service. VERITAS SHALL HAVE NO LIABILITY FOR ANY USE OF THE SDK FOR OTHER PURPOSES OR FOR ANY FAILURE OF THE SDK AND/OR THE SERVICE BASED ON CUSTOMER'S FAILURE TO PROPERLY DEVELOP, PROGRAM, INSTALL, CONFIGURE, OR MONITOR CUSTOMER'S INTEGRATION OF THE SERVICE WITH CUSTOMER'S EXISTING SYSTEMS, OTHER VERITAS PRODUCTS, OR THIRD-PARTY PRODUCTS. USE OF THE SDK IS SOLELY AT CUSTOMER'S RISK.

- Customer's right to use the SDK begins when an SDK license is purchased and ends when Customer's right to use the associated Service terminates or expires or purchased SDK license terminates or expires, whichever comes first. Thereafter, Customer must uninstall the SDK.

Customer Responsibilities

Veritas can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Veritas's performance of the Service may be delayed, impaired, or prevented and/or eligibility for Service Level Agreement benefits may be voided, as noted below.

- Setup Enablement: Customer must provide information required for Veritas to begin providing the Service.

- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the web portal interface, if applicable, or default settings will apply. In some cases, default settings do not exist, and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control.

- Configuration: Should a Service be suspended or terminated for any reason whatsoever, Veritas shall reverse all configuration changes made upon provisioning the Service and it shall be the responsibility of Customer to undertake all other necessary configuration changes when the Service is reinstated.

- Adequate Customer Personnel: Customer must provide adequate personnel to assist Veritas in delivery of the Service, upon reasonable request by Veritas.

- Web Interface Service Portal Access: Customer can access the Service portal by using a secure password protected login. The Service portal provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service. Customer must configure the features of the Service through the Service portal or default settings will apply. In some cases, default settings do not exist, and no Service will be provided until Customer chooses a setting. Configuration and use of the Service are entirely in Customer's control.

- Security: Customer shall perform commercially reasonable efforts, using procedures, third-party software, and the security features of the Service, to maintain the security of Customer Data.

- Compliance: Customer is responsible for all activities that occur in User accounts and for its Users' compliance with the Agreement and with the Acceptable Use Policy available at https://www.veritas.com/company/legal/acceptable-use-policy. If Customer becomes aware of a User's violation of the Agreement or Acceptable Use Policy, Customer must notify Veritas as soon as reasonably practicable.

- Security Vulnerability or Incident. If Customer becomes aware of any actual or potential security vulnerability or incident, Customer must immediately report it to Veritas through the process set forth at https://www.veritas.com/security or successor address.

Service-Specific Terms

Fair Use

Customers using the Service are expected to perform data operations and egress in line with normal and reasonable industry standards of similar services. Activities that fall outside of these reasonable standards include without limitation:

- data egress for purposes other than data recovery or responses to reasonable data privacy or eDiscovery requests
- egress of all data to populate another repository or because of Service cancellation
- excessive testing of backup or restoration capabilities

Should a Customer's usage result in excessive data operations or egress, Veritas reserves the right in its discretion to invoice for such excess use.

Assistance and Technical Support

Customer Assistance. Veritas will provide the following assistance as part of the Service:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support. The following technical support ("Support") is included with the Service.

- Support available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to address issues and questions with the Service.
- Support available for the Service does not include support for the SDK.

Maintenance. Veritas must perform maintenance on the Service Infrastructure in order to provide the Service in accordance with the Agreement. The following applies to such maintenance:

- *Planned Maintenance*. "**Planned Maintenance**" means scheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Veritas' standard Planned Maintenance time(s) are listed below. Veritas will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service.

- Veritas performs a weekly Planned Maintenance beginning at 12am GMT on Sundays and typically lasting for 2 hours or less. Customers that would like to alter this Planned Maintenance window will need to call Support to see if reasonable accommodations can be made.
- For any other Planned Maintenance outside of the above time(s), Veritas will use commercially reasonable efforts to give Customer five (5) calendar days' notification via the Service.

- *Emergency Maintenance.* "**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Veritas could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer. Where Emergency Maintenance is necessary and is likely to affect the Service, Veritas will endeavor to inform the affected parties in advance via email, or SMS or by phone no less than one (1) hour prior to the start of the Emergency Maintenance.

Automatic Renewal and Service Cancellation

Unless specified in the Agreement or Customer has otherwise opted out of auto-renewal at the time of initial purchase using Veritas' then-current opt-out processes, the Service renews automatically as set forth in the Agreement, unless Customer cancels as follows:

- Customer may opt out of automatic renewal, and therefore terminate, by providing Veritas notice of non-renewal or cancellation at least thirty (30) days prior to the end of Customer's Initial Period (sometimes called the Minimum Period) or a then-current Renewal Period (each, a "Term").
- Such notice of non-renewal or cancellation must be sent to the following address (or replacement address as published by Veritas): returnsandcancellations@veritas.com. For clarity, a notice of non-renewal or cancellation takes effect upon the expiration of the then-current Term and does not terminate the Service until the end of Customer's then-current term. Any notice given according to this procedure will be deemed to have been given when received.
- By submitting a non-renewal or cancellation notice, Customer acknowledges that Customer Data and its Customer Tenant will be permanently deleted in accordance with the Data Decommissioning section.

Please note that if Customer has opted out of auto-renewal at the time of purchase ("DNR"), Customer will be responsible for submitting a timely renewal order. Any processing delays, late renewals, channel issues or other problems with the renewal order may cause the Service to expire and any Customer Data stored by the Service shall be deleted in accordance with the

Data Decommissioning section. Not submitting a timely renewal order is deemed the same as a cancellation notice, and Customer Data and the Customer Tenant will be permanently deleted in accordance with the Data Decommissioning section.

Automatic renewals are subject to a renewal uplift, except that any renewal order of a DNR purchase or purchase provided under a promotional discount is subject to the then-current pricing.

Data Decommissioning

Customer Data will be decommissioned in the following events, or as otherwise set forth in this Service Description:

- Service cancellation (either by request of Customer or in the event of non-payment)
- Service termination or expiration
- License reduction at renewal in excess of 10%

Customer loses all access to the Service and its Customer Data, as well as any right to use the SDK, and no new backup jobs will be performed immediately following suspension, expiration, or termination of Services.

Unless otherwise prohibited by law or court order, decommissioned Customer Data will be deleted in accordance with our standard deletion practices within thirty (30) days of the Data Decommissioning event and is irretrievable thereafter.

If Customer needs a copy of their Customer Data, Customer should continue subscribing to the Service until such time as Customer has retrieved all Customer Data through self-service data exports.

Overages

If Customer's actual usage exceeds its contracted quantity, then Veritas will invoice for excess Service use and Customer will promptly pay for such excess use. In such an event, Veritas will charge fees for the excess use at the same rates for the current Term monthly in arrears or in accordance with Veritas' then-current processes.

Usage Reduction

Customer cannot reduce the agreed upon quantity of users or FETB during any existing term but may only reduce that quantity at renewal time. Absent evidence of a company divestiture, split or other entity realignment, Veritas reserves the right to reduce the quantities for the existing product(s) as a one-time courtesy by no more than ten percent (10%) of the existing amount at any given renewal time or as otherwise set forth in Veritas' then-current processes. Pricing will be adjusted for the lower volume which shall result in increased per user pricing, and prior discounting will not be available. Customer Data associated with the removed licenses will not be decommissioned but will count toward Customer's adjusted Shared Storage Allocation based on the new user and FETB quantities.

Additional Service Requirements

- Customer shall comply with all applicable laws with respect to use of the Service(s). In certain countries it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service(s) is entirely in

Customer's control, therefore, Veritas is not liable for Customer's use of the Service(s), nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

- Veritas may update the Service at any time in order to maintain the effectiveness of the Service.
- The Service (including any Software Components) may use open source and other third-party materials that are subject to a separate license. Please see the applicable Third-Party Notice, if applicable, at https://www.veritas.com/about/legal/license-agreements.
- Legacy Service Offerings: Service offerings listed in this Service Description are the ones generally available to new customers. For existing customers who may still be actively using a Service offering not detailed herein, please see https://www.veritas.com/content/dam/Veritas/docs/policies/Veritas_Alta_SaaS_Protection_Legacy_Service_Description.pdf for additional details on such Services.
- If Customer has not provided the requested provisioning information to allow Veritas to provide the Service, Veritas reserves the right to begin charging for the Service within thirty (30) days of receipt of an order for the Service.

Service Level Agreement ("SLA")

Veritas' Service Level Agreement is dependent on availability of the third-party cloud provider resources and is only available for customers where the Tenant is hosted in the Veritas Azure environment (i.e., a Veritas-Hosted Tenant).

- Veritas' Service Level Agreement shall provide 99.9% or higher Uptime for the Service.
- "Uptime" is defined as the time during which a Customer is able to Access the Service, as reported by the Veritas incident management system. "Access" is defined as a Customer being able to successfully login and use the Service functionality, as outlined in this Service Description.
- Uptime is measured every calendar month as a percentage value. The monthly Uptime percentage is the total number of minutes of Uptime achieved in a calendar month, divided by the total number of minutes in a calendar month.

Exclusions

- This SLA will not operate: (i) during periods of Planned Maintenance or Emergency Maintenance, periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) due to overall internet congestion, slowdown or unavailability; (iii) bandwidth or other limitations caused by Customer internet service provider (ISP); (iv) unavailability of generic internet services (e.g. DNS servers); (v) a result of Customer equipment or third party computer hardware, software or network infrastructure not within the sole control of Veritas; (vi) during any period of suspension of service by Veritas in accordance with the terms of the Agreement; (vii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (viii) Customer has not configured the Service in accordance with the Agreement.

Service Credits

- If the Service does not meet the stated SLA, Customer may submit a Service Credit Request for a Service Credit. Service Credits are calculated as follows:

Availability	Service Credit[1]
≥=99.9%	0%
>=99.0% but <99.9%	10%
<99.0%	25%

[1] Service Credits are calculated as a percentage of the monthly cost of the service when the outage occurred (regardless of licensing model). Service Credit percentages in the table above are an aggregate maximum for all SLA claims for a single Service in a given calendar month. Service Credits only apply if the Customer's account is current and not suspended for non-payment or other non-compliance with terms. Service Credits are provided to the party receiving the Veritas invoice.

- To successfully claim a Service Credit, Customer must submit a Service Credit Request within fifteen (15) business days of the end of the calendar month in which the suspected SLA non-compliance occurred. The request must specify which service was impacted, and the dates and times of service unavailability.

- Veritas will validate the information provided by the Customer and if a Service Credit is due, it will be applied against the next Veritas invoice for the Customer's Service. If a Service Credit is successfully claimed for more than one Veritas Service, then the quantity will equal the number of credits applied and the total will be aggregated to reflect the total value of the Service Credits claimed in that measurement period.

- The remedies set out in this SLA shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to this SLA.

Data Privacy

Data Collection; Data Protection Regulations. In connection with Customer's use of the Service, Veritas and Veritas' licensors, subcontractors, or agents on Veritas' behalf may collect, retain, disclose and use certain information ("Collected Data"). Collected Data may include, but is not limited to, personally identifiable information about Customer, Customer's devices or systems or Customer's software usage. Veritas uses such Collected Data to enable, optimize and provide the Service and/or maintenance/support to Customer (and may engage third parties to do so as well) and to improve Veritas' products and services in general, including by reviewing aggregate data for statistical analyses. By installing and/or using the Service, Customer agrees to allow Veritas to collect Collected Data as described in this section. Please refer to Veritas' product privacy notices at https://www.veritas.com/company/privacy in order to fully understand what information Veritas collects, retains, discloses, and uses from Customer or Customer's devices. Please note that the use of the Service may be subject to data protection laws or regulations in certain jurisdictions. Customer is responsible for ensuring that Customer's use of the Service is in accordance with such laws or regulations. Customer acknowledges that the Collected Data will be processed and accessible on a global basis by Veritas, its Affiliates agents and subcontractors for the purposes of providing the Service and/or maintenance/support, to generate statistical information about the Service, for internal research and development, and as otherwise described in the Agreement. Customer also consents for Customer and as agent for its contacts whose details have been collected as part of the Collected Data to the use by Veritas of that personal information for the purposes of informing Customer of Veritas products and services which may be of interest to Customer and account management. Where Customer's processing of the personal data provided to Veritas under this Agreement is subject to the General Data Protection Regulation (EU) 2016/679, or other applicable laws that relate to the processing of personal data and privacy that may exist in the European Economic Area, United Kingdom, or Switzerland, Veritas shall process such personal data in accordance with the Data Processing Terms and Conditions at www.veritas.com/privacy. Veritas may disclose the Collected Data as required or permitted by law or in response to a subpoena or other legal process.

Definitions

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Service Description, have the meaning given below:

"**Azure**" means the Microsoft cloud infrastructure and platform offering known as "Azure".

"**Customer Data**" means the data Customer stores or archives in the Service.

"**FETB**" or "**Front-End Terabyte**" means front-end terabyte and refers to the total aggregate amount of uncompressed data in terabytes. One terabyte equals 1,024 gigabytes of data.

"**GB**" refers to the total aggregate amount of uncompressed data in gigabytes. One gigabyte equals 1024 megabytes of data.

"**Infrastructure**" means any Veritas or licensor technology and intellectual property used to provide the Services.

"**Open Source Code**" means a software program that is licensed under terms that require disclosure to parties other than the licensor of the source materials of the software program or modifications thereof, or any source materials of any other software program with which the Open Source Code software program is intended to operate, or that create obligations to distribute any portions of any software program with which the Open Source Code software program is used. Open Source Code includes, without limitation, any software licensed under the GNU General Public License.

"**Service Component**" means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Veritas as an incidental part of a Service. Any additional rights and obligations with respect to the use of Service Components shall be as set forth in this Service Description.

“Service Credit” means the amount of money that will be credited to Customer’s next invoice after submission of a Service Credit Request and validation by Veritas that a credit is due to Customer.

“Service Credit Request” means the SLA credit request a Customer submits to Veritas by creating a technical support case. Information on how to create a technical support case may be found at https://www.veritas.com/support/en_US.html.

“**Software Component**” means a Service Component consisting of Veritas software in object code format, as may be required by a Service, which must be installed by Customer outside of the Tenant, in order to receive the Service, or some portion thereof.

“**Subscription Instrument**” means one or more of the following applicable documents which further defines Customer’s rights and obligation related to the Service: a Veritas certificate or a similar document issued by Veritas, or a written agreement between Customer and Veritas, that accompanies, precedes or follows the Service.

“**Subscription Period**” means the period beginning from execution of a Subscription Order Form and ending upon termination or cancellation of the Service.

“**Structured Data**” means data that conforms to a data model, has a well-defined structure, follow a consistent order, and can be accessed and used by a computer program. For purposes of illustration only: machine generated data, event logs, database records.

“Suite” means a collection of Veritas Alta Archiving Services sold together as detailed further in this Service Description.

“**Tenant**” means the isolated compute, storage, and networking resources and related configuration that is hosted in a cloud environment that is dedicated to Customer. A Tenant hosted by Veritas is known as a “Veritas-Hosted Tenant.”

“**Unstructured Data**” means data that is not Structured Data. For purposes of illustration only: video, images, audio, user-generated files, application data, compliance records, litigation data, and public records data.

“**User**” means an individual who is authorized by Customer to use the Service.