VMWARE CLOUD SERVICES GUIDE

Date: 17 August 2022

Table of Contents

1. TERMS APPLICABLE TO ALL VMWARE CLOUD SERVICES

The terms set forth in this VMware Cloud Services Guide ("**Cloud Services Guide**") apply to all Cloud Services, as provided in the VMware General Terms ("**General Terms**") and the Cloud Services Exhibit to the General Terms ("**Cloud Exhibit**"), available at www.vmware.com/agreements. Terms used but not defined in this Cloud Services Guide have the meanings set forth in the General Terms and the Cloud Exhibit. Individual services may have additional or differing provisions for any of the terms included in this Section 1; refer to the individual service entries in Section 2.

SERVICE OPERATIONS DATA

In connection with providing a Cloud Service, VMware collects and processes information (such as configuration, performance, and log data) from VMware's software or systems hosting the Cloud Service, and from Customer's systems, applications, and devices that are used with the Cloud Service. This information is processed to facilitate delivery of the Cloud Service, including but not limited to (i) tracking entitlements, (ii) providing support, (iii) monitoring and ensuring the performance, integrity, and stability of the Cloud Service's infrastructure, and (iv) preventing or addressing service or technical issues. To the extent any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with VMware's Privacy Notices, including the VMware Products and Services Notice available at: https://www.vmware.com/help/privacy.html

USAGE DATA

The Cloud Service collects data (such as configuration, performance, and usage data) directly from VMware's software or systems hosting the Cloud Service, and from Customer's systems, applications, and devices involved in the use of the Cloud Service, to improve VMware products and services, and Customer's and its Users' experiences, as more specifically described in VMware's Trust & Assurance Center at https://www.vmware.com/solutions/trustvmware/usage-data-programs.html. With respect to user-entered values within configuration object names such as the machine names, host names or dashboard names, Customer should not name those systems using confidential or personal data.

To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with VMware's Privacy Notices, including the VMware Products and Services Notice available at: https://www.vmware.com/help/privacy.html.

In connection with the collection of usage data, VMware and its service providers use cookies. Detailed descriptions of the types of cookies VMware uses can be found in VMware Privacy Notices available at https://www.vmware.com/ help/privacy.html. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can also be found from that link.

DELETION OF DATA

Following the end of the Subscription Term, (i) Customer Content will be deleted not later than 90 days after the effective termination date, and (ii) all personal data in VMware's possession regarding Customer's use of the Cloud Service will be deleted from VMware's primary database and (if applicable) back-up database, except to the extent VMware is required by applicable law to retain some or all of the personal data (in which case VMware shall implement reasonable measures to isolate the personal data from any further processing). VMware retains anonymized and hashed data.

DATA COLLECTION BY GOOGLE ANALYTICS

Some Cloud Services may utilize Google Analytics to collect data directly from any browsers used to view or receive the Cloud Service. The data collected and inferred is used by VMware to diagnose and improve its products and services and to fix issues. Further information on how Google collects and uses this data when customers use a Cloud Service can be found at: www.google.com/policies/privacy/partners/.

This data collection is made possible by the use of cookies. Detailed descriptions of the types of cookies VMware uses can be found in the VMware Privacy Policy and policies linked from that Privacy Policy. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can also be found from that link. Customer agrees to provide the information in this section to its Users.

CLOUD SERVICE OPERATIONS

The following outlines VMware's general roles and responsibilities in providing a Cloud Service. While specific roles and responsibilities have been identified as being owned by Customer, any roles or responsibilities not contained in this Cloud Services Guide are either not the duty of VMware or are assumed to be Customer's responsibility.

Service Provisioning

VMware will provide the following provisioning services. Specific Cloud Services may have different requirements.

- VMware will create an instance of the service for Customer.
- VMware will create a corresponding service account and send an email or other notification to the contact that Customer identified in the Order inviting that contact to the newly created instance. A URL to access the service will be provided within that notification.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.

Customer's responsibilities include:

- Deploying and configuring data agents and the proxy to collect and route data into the service as needed.
- Configuring the service to gather metrics from cloud-based services (for example, Amazon Web Services) as needed.

Incident and Problem Management

VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which VMware has direct, administrative access and control, including servers and services used to provide the Cloud Service.

Customer is responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Customer's account settings in the Cloud Service administrative management console.
- User-deployed and user-configured assets such as proxy agents.
- Anything else not under VMware's direct control and administration.

Change Management

VMware will provide the following change management elements:

- Processes and procedures to release new code versions and bug fixes.

Customer is responsible for:

- Management of changes to Customer's tagging process, alert settings, dashboards, and other content.
- Administration of self-service features provided through the Cloud Service's system console and user portal, up to the highest permission levels granted to Customer.
- Changes in the data collection agents used.
- Cooperating with VMware when planned or emergency maintenance is required.

Security

The end-to-end security of the Cloud Service is shared between VMware and Customer. The primary areas of responsibility between VMware and Customer are outlined below.

VMware will use commercially reasonable efforts to implement reasonable and appropriate measures designed to help Customer secure Customer Content against accidental or unlawful loss, access, or disclosure, including the following:

- Information Security: VMware will protect the information systems used to deliver the Cloud Service over which VMware (as between VMware and Customer) has sole administrative level control.
- Security Monitoring: VMware will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Cloud Service over which VMware (as between VMware and Customer) has sole administrative level control. This responsibility stops at any point where Customer has some control, permission, or access to modify an aspect of the Cloud Service.
- Patching and Vulnerability Management: VMware will maintain the systems VMware uses to deliver the Cloud Service, including the application of patches VMware deems critical for the target systems. VMware will perform routine vulnerability scans to surface critical risk areas for the systems VMware uses to deliver the Cloud Service. Critical vulnerabilities will be addressed in a timely manner.

Customer is responsible for addressing the following:

- Information Security: Customer is responsible for ensuring adequate protection of the content that Customer deploys and/or accesses with the Cloud Service. This includes, but is not limited to, any level of virtual machine patching, security fixes, data encryption, access controls, roles and permissions granted to Customer's internal, external, or third party users, etc.
- Network Security: Customer is responsible for the security of the networks over which Customer has administrative level control. This includes, but is not limited to, maintaining effective firewall rules in all software-defined data centers ("**SDDCs**") that Customer deploys in a Cloud Service.
- Security Monitoring: Customer is responsible for the detection, classification, and remediation of all security events that are isolated with Customer's deployed SDDCs, associated with virtual machines, operating systems, applications, data, or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which Customer is required to participate, and which are not serviced under another VMware security program.

AUTHORIZATIONS, COMPLIANCE

The VMware Cloud Trust Center, at https://www.vmware.com/products/trust-center.html#overview, provides information about security, privacy, compliance, and resiliency of VMware Cloud Services. The section on compliance programs lists VMware offerings that have achieved or are pursuing certification or authorization for specific programs (e.g., FedRAMP) are listed for the various programs. If an offering is not listed, then the offering is not certified or authorized for the particular program, nor is certification or authorization being pursued.

2. CLOUD SERVICES

2.1 CLOUDHEALTH® BY VMWARE SUITE™

Overview: CloudHealth® by VMware Suite™ is a cloud service management platform that collects and consolidates a customer's cloud environment data by gathering data and metadata related to the customer's use of cloud-based services.

Google Analytics: CloudHealth by VMware utilizes Google Analytics.

Data Retention and Deletion:

During the Subscription Term, data transmitted to the Cloud Service by Customer will be retained and available for querying and alerts. Data is retained for 13 months from the date and time the data was originally ingested into the Cloud Service.

VMware will retain Customer Content in VMware's backup systems for 90 days following the effective termination date of the Subscription Term. If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify VMware within thirty (30) days after the effective termination date, and VMware will assist Customer in extracting Customer Content from the Cloud Service. Customer is responsible for all fees associated with Customer Content extraction. If Customer does not notify VMware within the 30-day period, Customer Content will be permanently deleted and will not be recoverable.

2.2 CLOUDHEALTH® SECURE STATE™

Overview: CloudHealth® Secure State™ is a cloud security monitoring service that looks across configuration settings, configuration change activity, and threat events to help detect vulnerabilities and find suspicious activity in public cloud environments. (As of the date of this Service Guide, CloudHealth Secure State is compatible with Amazon Web Services and Microsoft Azure public cloud environments.)

Free Tier Offering:

The service includes CloudHealth Secure State Free Tier ("**Free Tier**"), a free of charge, limited scope offering available as part of Customer's use of the CloudHealth Secure State. The Free Tier offering includes the following feature limitations.

- Cloud resources under monitoring are limited to the ones belonging to one public cloud account
- Kubernetes resources are limited to one attached Kubernetes cluster
- Limited inventory refresh frequency (maximum once daily)
- Real-time inventory updates based on change events are not available
- Custom rules and custom frameworks are not available
- Integrations are limited to email and slack
- Reports, Projects, Remediation, and third-party findings are not available
- Limited support (community forum / bug reporting)

VMware will monitor Free Tier accounts for use that may degrade the Cloud Service, or that circumvents or attempts to circumvent the use limitations of the Free Tier offering. VMware may terminate Customer's and/or any User's access to the Free Tier account for any such use. VMware reserves the right to end the Free Tier offering any time.

Data Retention and Deletion:

During the Subscription Term, data transmitted to CloudHealth Secure State by Customer will be retained and available for querying and alerts for 13 months from the date and time the data was originally ingested into the service.

Customer's CloudHealth Secure State environments, configurations, and data collected by the Cloud Service specific to cloud configuration, change events, and object metadata will be deleted from VMware systems (including VMware backup systems) within 90 days after the Subscription Term ends.

2.3 UHANA™ BY VMWARE

Overview: Uhana™ by VMware uses artificial intelligence-based analytics to provide mobile network operators the ability to generate actionable insights from their 4G and 5G radio access networks to improve customer experience and reduce operational costs.

Although the Cloud Service is installed in Customer's environment, it is managed by VMware. Customer has no right to take possession of the software elements of the Cloud Service installed in its environment. The Cloud Service can only be managed and operated by VMware; Customer cannot manage and operate the Cloud Service, nor can Customer have any party other than VMware manage and operate the Cloud Service.

2.22 VMWARE APPLICATION CATALOG™

Overview: VMware Application Catalog™ allows customers to define catalogs that are delivered to a private repository ("**artifacts repository**"). A "**catalog**" consists of a set of applications, built on top of a golden image (Customer-provided or VMware-provided) for a specific deployment format (e.g., Helm Chart). Once a catalog is defined and delivered, it will be updated whenever new versions of the applications are available. Additional details and reports for each delivered version of an artifact are accessible through the service's user interface ("**UI**") at https://app-catalog.vmware.com. For purposes of this Cloud Services Guide, all applications provided through VMware Application Catalog are considered "Third-Party Content", as defined in the General Terms. For United States federal, state, and local government customers, the UI is not supported. Both artifacts and reports are delivered to a VMware-provided private repository.

Data Retention and Deletion:

After termination of the Subscription Term, all content, and all personal data contained in content, in VMware's possession will be retained for six months; provided, however, Customer can request deletion prior to the end of the six-month retention period. After the end of the retention period, Customer Content and personal data will be deleted from VMware's primary database and (if applicable) back-up

2.4 VMWARE CARBON BLACK CLOUD™

Overview: VMware Carbon Black Cloud™ is a cloud-native Endpoint and workload protection platform that enables customers to protect, prevent, detect, and respond to cybersecurity attacks on their Endpoints and server workloads.

The Agreement supersedes any terms that may be presented to Customer upon logging into the service.

For VMware Carbon Black® Cloud Managed Detection™ (formerly known as CB ThreatSight) and VMware Carbon Black® Cloud Managed Detection and Response ("**MDR**"), any warranties in the General Terms and the Cloud Exhibit are expressly excluded. The sole and exclusive warranty for VMware Carbon Black Cloud Managed Detection and MDR, express or implied, is as follows: VMware Carbon Black warrants that VMware Carbon Black Cloud Managed Detection and MDR

will be performed in a professional and workmanlike manner consistent with industry standards for similar types of services.

Google Analytics: VMware Carbon Black Cloud utilizes Google Analytics.

Definitions: For purposes of this Section 2.4 and Section 2.5, the following terms have the following meanings:

"Core" means a unit of measure that is defined based on the environment in which the product operates: (1) in a physical computing environment, a Core is a Physical Core; (2) in a virtualized or hypervisor (VM) computing environment, a Core is a single physical computational unit of the Processor which may be presented as one or more vCPUs; and (3) in a public cloud computing environment, a Core is defined as a single physical computational unit of the Processor, which may be presented as one or more vCPUs, but which may be named differently by the public cloud vendors. In cases where these proxies are not identified as Hyperthreads, one (1) proxy is recognized as one Core. In cases where these proxies are identified as Hyperthreads, two (2) proxies are recognized as one Core. All Cores existing in an environment must be covered by appropriate entitlements.

"Endpoint" means the computer device(s) on which the Sensor Software is installed, including but not limited to laptops, desktops, tablets, point of sale devices, and servers.

"Hyperthread" means a technology by which a single physical core is shared between two logical cores.

"Node" means a single host/OS that runs containers. A Node can be a virtual or a physical machine.

"Physical Core" means a single physical computational unit of the Processor.

"Processor" means a single, physical chip that houses at least one, but not more than 32, Physical Cores that can execute computer programs. A physical chip containing more than 32 Physical Cores requires the purchase of one additional subscription for every additional 32 (or portion thereof) Physical Cores in the Processor.

"Sensor Software" means software agents installed on a customer's Endpoints or workloads.

"Virtual CPU" or "vCPU" means a single unit of virtual processing power configured to a Virtual Machine.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a physical machine.

The Sensor Software is subject to the General Terms and the Software Exhibit, which supersede any conflicting terms that may be presented to Customer upon logging into VMware Carbon Black Hosted EDR.

Additional Terms:

Threat Intelligence Data Collection

Certain VMware Carbon Black Cloud services may collect data relating to malicious or potentially malicious code, binaries, attacks, activities, and vulnerabilities on a customer's Endpoints or workloads ("Threat Intelligence Data"). Threat Intelligence Data is collected by VMware for analysis and possible inclusion in a threat intelligence feed utilized by certain VMware Carbon Black services. Prior to inclusion in any threat intelligence feed, Threat Intelligence Data will be: (i) reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in the customer's systems and other customers' systems and/or (ii) be anonymized and made un-attributable to any particular customer or individual (collectively "Un-attributable Threat Intelligence Data"). VMware may distribute Un-attributable Threat Intelligence Data to its customers at its discretion as part of its threat intelligence data feed or in published reports or research. By using a VMware Carbon Black Cloud service, Customer is deemed to have agreed that Un-attributable Threat Intelligence Data is not Customer Content, and VMware may retain, use, copy, and modify the Threat Intelligence Data for its internal business purposes, and additionally distribute and display the Un-attributable Threat Intelligence Data, for its business purposes, including without limitation for developing, enhancing, and supporting products and services, and for use in its threat intelligence feed or in published reports and research. The information provided via any threat intelligence feed is provided on an "AS IS" and "AS AVAILABLE" basis only.

Updates and Upgrades to Sensor Software

VMware may release patches, bug fixes, updates, upgrades, maintenance and/or service packs ("**Updates**") for the Sensor Software from time to time, which may be necessary to ensure the proper function and security of the VMware Carbon Black Cloud services. VMware is not responsible for performance, security, warranty breaches, support or issues encountered in connection with the VMware Carbon Black Cloud services that result from Customer's failure to accept and apply Updates within a reasonable time frame.

Usage Data

Customer agrees to provide the information in this Cloud Services Guide, including this Section 2.4, regarding the collection and use of usage data, including any available controls in relation to the cookies or tracking technology, including those provided by third parties, to all users of the VMware Carbon Black services.

Customer Responsibilities

Customer must maintain accurate records of its use of the Sensor Software during the Subscription Term, and for 12 months after the effective termination date of the Subscription Term, sufficient to show compliance with the Agreement. VMware has the right to audit those records. Any audit will be subject to reasonable prior notice and will not unreasonably interfere with Customer's business activities. VMware may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. Customer must reasonably cooperate with VMware and any third-party auditor and Customer must, without prejudice to VMware's other rights, address any non-compliance identified by the audit by paying any additional fees required as a result of that non-compliance. Customer must reimburse VMware for all reasonable costs of the audit if the audit reveals either underpayment of more than five (5%) percent of the fees payable by Customer for the period audited, or that Customer has materially failed to maintain accurate records of Sensor Software use.

Data Retention and Deletion:

During the Subscription Term, data will be retained and deleted as set forth below.

VMware Carbon Black Cloud Endpoint™ Standard:

- Short term events are retained and available to Customer for a minimum of 30 days and a maximum of 32 days for search and investigation.
- Alerts and their associated event data ("long term events") are retained for a minimum of 180 days and a maximum of 210 days.

VMware Carbon Black Cloud® Enterprise EDR™:

- Endpoint data is stored for 30 days in the following two formats: (1) proprietary format for endpoint data optimized for fast retrieval, and (2) Solr indices.
- Raw protobufs (for troubleshooting purposes) are stored for 7 days.

VMware Carbon Black Cloud® Audit and Remediation™:

- The past query list is retained for 30 days.
- The results of a query are retained for 30 days (VMware stores up to 7,500 results per Endpoint per day). A User can choose to export the results on the User's own device.

Live Response Feature

- Using the Live Response feature, the administrator may remote into a device to take an action. If the action involves getting a copy of a file, the file is temporarily captured in the session cache for the duration of the Live Response session and in any event is automatically deleted after 15 minutes of inactivity. This time frame is configurable.

Log Data

- During the Subscription Term, diagnostic logs are purged after seven days and audit logs are removed every 12 months.

If Customer wishes to extract Customer Content from the VMware Carbon Black Cloud service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify VMware within five (5) days after the effective termination date, and VMware will assist Customer in extracting Customer Content from the VMware Carbon Black

Cloud service. Customer is responsible for all fees associated with content extraction. If Customer does not notify VMware within that five-day period, Customer Content will be permanently deleted and may not be recoverable.

2.5 VMWARE CARBON BLACK® HOSTED EDR™

Overview: VMware Carbon Black® Hosted EDR™ (formerly known as CB Response Cloud) is a highly scalable incident response and threat hunting solution designed for security professionals and security operations center (SOC) teams. Carbon Black Hosted EDR continuously records and stores unfiltered Endpoint data, so that SOC professionals can proactively detect advanced threats, hunt threats in real time, and visualize the complete attack kill chain. The service leverages the VMware Carbon Black Cloud™ aggregated threat intelligence functionality, which is applied to the Endpoint activity system of record for evidence and detection of these identified threats and patterns of behavior.

The Sensor Software is subject to the General Terms and the Software Exhibit, which supersede any conflicting terms that may be presented to Customer upon logging into VMware Carbon Black Hosted EDR.

Additional Terms:

Disclosure of Personal Data

VMware will not disclose personal data outside of VMware or its affiliates except: (i) as Customer directs; (ii) as described in the Agreement; or (iii) as required by law. VMware Carbon Black Hosted EDR may include optional functionality provided by third party processors. If Customer chooses to utilize that functionality, Customer will be provided advance notice of the processing details. Following that notification, Customer may choose to: (a) refrain from utilizing the applicable functionality, in which case such processing will not occur; or (b) proceed with the functionality, in which case VMware will be authorized to process in accordance with the details provided.

Threat Intelligence Data Collection

Carbon Black Hosted EDR may collect data relating to malicious or potentially malicious code, attacks, and activities on Customer's Endpoints ("**Threat Intelligence Data**"). Threat Intelligence Data is collected by VMware for analysis and possible inclusion in a threat intelligence feed utilized by certain VMware Carbon Black services. Prior to inclusion in any threat intelligence feed, Threat Intelligence Data will be: (i) reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in Customer's systems and other customers' systems; and/or (ii) be anonymized and made un-attributable to any particular customer or individual. VMware may distribute Threat Intelligence Data to its customers at its discretion as part of its threat intelligence data feed. By using a VMware Carbon Black service, Customer is deemed to have agreed that Threat Intelligence Data is not Customer Data, and VMware may retain, use, copy, modify, distribute and display the Threat Intelligence Data for its business purposes, including without limitation for developing, enhancing, and supporting products and services, and for use in its threat intelligence feed. The information provided via any threat intelligence feed is provided on an "AS IS" and "AS AVAILABLE" basis only.

Updates and Upgrades to On-Premises Components

VMware may release patches, bug fixes, updates, upgrades, maintenance and/or service packs ("**Updates**") for the Sensor Software from time to time, which may be necessary to ensure the proper function and security of the service. VMware is not responsible for performance, security, warranty breaches, support or issues encountered in connection with the service resulting from Customer's failure to accept and apply Updates within a reasonable time frame.

2.3 VMWARE CLOUD™

Overview: VMware Cloud™ is a multi-cloud service for all apps across data center, edge, and public cloud environments. VMware Cloud enables modular, multi-cloud infrastructure, app, and management services that accelerate app modernization and cloud transformation to deliver innovation for customers. VMware Cloud platform includes general services, infrastructure services, integrated services, and solutions.

Customers gain access to VMware Cloud through a VMware Cloud Services invitation, which enables them to establish their cloud services organization. After organization creation, customers arrive at the VMware Cloud Console. The VMware Cloud Console provides access to infrastructure services, integrated services, and solutions, all of which have their own service provisioning methods. Customers can create additional user accounts as needed.

Google Analytics: VMware Cloud utilizes Google Analytics.

Data Retention and Deletion:

Data retained in VMware Cloud pertains only to the meta-data associated with customer deployments for inventory, subscriptions, and other service data. There is no actual customer data or Customer Content from any infrastructure deployments.

The VMware Cloud Console data, including any configuration information for infrastructure services, integrated services, and solutions, and any data that VMware collects relating to Customer's use of VMware Cloud, persists in the AWS US-West (Oregon) data center location, but may be replicated to other AWS regions to ensure availability of VMware Cloud.

2.6 VMWARE CLOUD DIRECTOR™ SERVICE

Overview: The VMware Cloud Director™ service enables cloud providers, managed service providers, and approved VMware customers who are not participants in the appropriate VMware partner program (each, a "**Cloud Provider**") to deploy instances of the VMware Cloud Director service ("**Cloud Director Instances**" or "**CDIs**") in a self-service manner to multiple regions across the globe. The Cloud Provider deploys and monitors CDIs through the service platform.

Data Retention and Deletion:

VMware retains Customer Content in its backup systems for three (3) days following the effective termination date of the Subscription Term. If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify VMware within 24 hours after the effective termination date, and VMware will assist Customer in extracting Customer Content from the Cloud Service. Customer is responsible for all fees associated with content extraction. If Customer does not notify VMware as required, Customer Content will be permanently deleted and will not be recoverable.

2.8 VMWARE CLOUD DISASTER RECOVERY™

Overview: VMware Cloud Disaster Recovery™ can be used to protect a customer's VMware vSphere® virtual machines by replicating them periodically to the cloud and recovering them as needed to a target VMware Cloud™ on AWS SDDC. The target SDDC can be created immediately prior to performing a recovery and does not need to be provisioned to support the replications in the service's steady state.

Additional Terms:

Restrictions on Use: To facilitate quick recovery of the protected virtual machines to a VMware Cloud on AWS SDDC, VMware Cloud Disaster Recovery automatically creates one or more NFS

datastores and attaches them to the SDDC. Using these datastores, the recovery of the virtual machines can be initiated immediately, with the virtual disk backups still residing on the SCFS. The virtual machines can also run directly off these datastores – also referred to as the "**Live Mount**" – for a period of time while the virtual disk backup data is automatically copied in the background to the VMware vSAN™ datastore on the SDDC. These NFS datastores are created exclusively for the purpose of exposing the virtual machine backups to the SDDC to facilitate disaster recovery and should never be used as general-purpose storage. Customer must not, and is not permitted to, use the vSphere Client, vSphere APIs, or any method other than the interfaces provided by VMware Cloud Disaster Recovery to create and power on virtual machines directly on these NFS datastores except through capabilities and workflows exposed in the service. If this restriction is not adhered to, VMware will not guarantee support for the affected instances of the service.

PCI Compliance: VMware Cloud Disaster Recovery is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. The compliance assessment was conducted by Crowe LLP, an independent Qualified Security Assessor (QSA). After initial deployment of the Service Offering, you must affirmatively take steps to configure your environment to meet your responsibilities as described in the Shared Responsibility Model, at: https://core.vmware.com/resource/vmware-cloud-disaster-recovery-shared-responsibility-model

You should make sure that the VMware Cloud on AWS SDDC used with service for recovering your virtual machines is PCI hardened, which might require disabling several VMware Cloud on AWS SDDC add-on capabilities in order to maintain compliance, including VMware HCX®. VMware will provide a customer-facing website, listing compliant offerings, that you can reference to ensure that you disable non-compliant VMC add-ons to maintain PCI compliance for your VMC on AWS environment. In addition, once a VMware Cloud on AWS SDDC is configured for PCI compliance, the networking and security configuration can be managed by you directly via the VMware NSX® Manager™ deployed in the SDDC rather than by the VMC Console.

For more details, refer to the documentation at docs.vmware.com. See the following for VMware Cloud on AWS Regions that are available for deployment of PCI compliant SDDCs: https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-19FB6A08-B1DA-4A6F-88A3-50ED445CFFCF.html

Before deploying any other VMware service in your instance of VMware Cloud Disaster Recovery, you should review the interoperability and compliance information for that other service. See https://cloud.vmware.com/trust-center/compliance for the most current information on compliant offerings. You are responsible for ensuring that any additional service deployed in your VMware Cloud Disaster Recovery instance meets your compliance and security requirements.

Data Retention and Deletion:

Customer Content stored within the service will be permanently deleted within five to 10 calendar days after the effective termination date of the Subscription Term and will not be recoverable after that time.

2.9 VMWARE CLOUD™ ON AWS

Overview: VMware Cloud™ on AWS brings VMware's enterprise class SDDC offering to the Amazon Web Services cloud, enabling customers to run any application across vSphere-based private, public, and hybrid cloud environments. VMware Cloud on AWS is a software-as-a-service offering that allows customers to deploy SDDCs running vSphere, NSX, and vSAN on Amazon Web Services.

Additional Terms:

Amazon Web Services Account

Customer will not be able to access or use VMware Cloud on AWS without having its own AWS customer account (an "**AWS account**"), which Customer must establish directly with AWS. This means that if Customer does not already have an AWS account, Customer must establish one

prior to being able to access the VMware Cloud on AWS service. Prior to provisioning an SDDC, VMware requires customers to connect to their AWS account. This process establishes identity and access management policies in Customer's AWS account that enable communication between resources provisioned in Customer's AWS account and in the SDDC.

Microsoft Server Products

If Customer is running Windows workloads in Customer's VMware Cloud on AWS service instance and wishes to leverage the functionality of the Microsoft Windows Server Datacenter offering or the Microsoft SQL Server Enterprise offering (collectively, the "Microsoft Products"), Customer may have VMware enable the Microsoft Products, under VMware's own licenses for the Microsoft Products, for Customer's environment. VMware is a licensee of the Microsoft Products pursuant to a separate agreement between Microsoft and VMware. Customer may be able to provision its existing license(s) in Customer's environment, if those licenses are eligible for that portability, pursuant to Customer's own license agreement with Microsoft. If Customer elects to have VMware enable the Microsoft Products for Customer's VMware Cloud on AWS instance, VMware will charge Customer for this use.

Customer's use of the Microsoft Products is subject to the following conditions, which are in addition to the provisions of the Agreement:

1. The Microsoft Products may only be used with Customer's instance of the VMware Cloud on AWS service. Customer is not permitted to provision or to allow anyone else to provision the Microsoft Products in any other environment, including but not limited to Customer's on-premises environment.
2. The Microsoft Products may not be used in high-risk activities, as described in the General Terms.

3. Customer may not remove, modify, or obscure any copyright, trademark, or other proprietary rights notices that are contained in or on the Microsoft Products.
4. Customer may not reverse engineer, decompile, or disassemble the Microsoft Products, except to the extent that such activity is expressly permitted by applicable law.
5. Microsoft, to the extent permitted by applicable law, disclaims all warranties regarding, and any liability on the part of Microsoft or its suppliers for, any damages, whether direct, indirect, or consequential, arising from Customer's use of VMware Cloud on AWS.
6. The Microsoft Products are the intellectual property of Microsoft. Customer's rights to use the Microsoft Products are limited to those rights expressly granted in the Agreement and are subject to the conditions in this section ("**Microsoft Server Products**").
7. Microsoft is a third party beneficiary of these terms, with the right to enforce these terms and to verify Customer's compliance with these terms.

If Customer needs support for the Microsoft Products, Customer must contact Microsoft, or Customer's preferred third-party support provider. VMware will not provide support for the Microsoft Products that Customer uses in connection with its Service Offering instance.

NOTE: The separate license agreement between VMware and Microsoft regarding the Microsoft Products requires VMware and/or Customer's authorized VMware channel partner to disclose Customer's name and address to Microsoft, and Customer acknowledges this and consents to this disclosure, (i) if Customer has a demonstration of the VMware Cloud on AWS service, using the Microsoft Products, or (ii) if Customer uses the VMware Cloud on AWS service on a trial or evaluation basis and the Microsoft Products are used. If Customer elects to have VMware provision the Microsoft Products in Customer's VMware Cloud on AWS service instance, VMware is also required to disclose to Microsoft the country in which Customer's instance of the service is provisioned, and Customer acknowledges and consents to this disclosure. This information will be used by Microsoft to verify VMware's compliance with the terms of the separate license agreement between VMware and Microsoft regarding the Microsoft Products, and Customer's compliance with the terms set forth above in this section ("**Microsoft Server Products**").

PCI Compliance:

VMware Cloud on AWS is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA). After initial deployment of an SDDC, Customer may choose to configure the SDDC for PCI compliance. Once configured for PCI, Customer must affirmatively take steps to disable several SDDC add-on capabilities in order to maintain compliance, including VMware HCX®. VMware will provide a customer-facing website, listing compliant offerings, that Customer can reference to ensure that Customer disables non-compliant add-ons to maintain PCI compliance for Customer's VMware Cloud on AWS environment. In addition, once an SDDC is configured for PCI compliance, the Networking and Security configuration will be managed directly via the VMware NSX® Manager™ deployed in the SDDC rather than by the VMware Cloud console. For more details, refer to the documentation at docs.vmware.com. The following VMware Cloud on AWS regions are available for deployment of PCI compliant SDDCs: US East (Northern Virginia).

Before deploying any other or add-on VMware service in Customer's instance of the VMware Cloud on AWS service, Customer should review the interoperability and compliance information for the service. See https://cloud.vmware.com/trust-center/compliance for the most current information on compliant offerings. Customer is responsible for ensuring that any additional service deployed in Customer's VMware Cloud on AWS instance meets Customer's compliance and security requirements.

Google Analytics: VMware Cloud on AWS utilizes Google Analytics.

Use of FullStory:

VMware Cloud on AWS uses FullStory functionality to collect data directly from any browsers used to access and use the service. FullStory collects data regarding use of the service, including user interaction and behavior, to enable session replay. The data collected and inferred is used by VMware to diagnose and improve its products and services, and to address issues. For users who wish to opt out of session recording, FullStory makes the following website available: https://www.fullstory.com/optout/.

Capacity Management:

Customer is responsible for capacity management of its SDDCs. VMware requires that 30% unused space ("**slack space**") be maintained in the VMware vSAN™ datastore within the service, to support operation of the SDDC. Adequate slack space is required for use of the vSAN datastore. If storage free space reaches (or falls below) 25%, it is possible that Customer could lose the ability to utilize the SDDC, and the environment could become inoperable. If unused space in an SDDC vSAN datastore drops reaches (or falls below) 25%, VMware will automatically add hosts to the SDDC to prevent damage to the SDDC. Customer can use the VMware Cloud sizer tool, found at https://vmcsizer.vmware.com/home, for guidance on the appropriate number of hosts needed to support anticipated workloads.

If Customer has changed the Elastic DRS for VMware Cloud™ on AWS (Elastic Distributed Resources Scheduler) ("**eDRS**") policy to "Optimize for Best Performance" or "Optimize for Lowest Cost", VMware will automatically size Customer's SDDC up or down based on load and according to the eDRS policy Customer has chosen. If Customer does not change the eDRS settings, the default option is "Scale Up for Storage Only" which means that VMware will add hosts to Customer's SDDC only when storage capacity becomes critical (that is, 25% or less free space). When eDRS is set to "Scale Up for Storage Only" VMware will not automatically scale down the SDDC.

Unless VMware and Customer otherwise agree, additional hosts added pursuant to this capacity management process will be billed at the then-current published on-demand rate for as long as those hosts are provisioned.

Data Retention and Deletion:

Retention and storage policies associated with Customer Content in the VMware Cloud on AWS service (including any personal data in Customer Content) are solely managed by Customer. VMware does not back up Customer Content in the service and therefore will not be able to recover any Customer Content in any unforeseen event.

Customer is responsible for implementing tools, products, and operational procedures to support data migration, data protection, backup/archive, and restoration for all Customer Content and all configurations created by Customer in the SDDC, including Virtual Machines and Content Libraries.

Termination of Customer's VMware Cloud on AWS instance will result in permanent loss of access to the environments, discontinuation of services, and a deletion of the environments and configurations pursuant to VMware practices. Any deletion of a host on VMware Cloud on AWS results in an automated cryptographic wipe of the hard drive, that is performed via destruction of keys used by the self-encrypting drives. This cryptographic erasure ensures that there is no Customer Content on the drives before returning the hosts to the pool of available hardware to be reprovisioned or decommissioned.

Service Operations Data and Usage Data is backed up by VMware. A storage policy enforces retention of three years and automatically purges log events that exceed the three-year lifecycle.

2.10 VMWARE CLOUD™ ON AWS GOVCLOUD (US)

Overview: The VMware Cloud™ on AWS GovCloud (US) cloud service offering brings VMware's enterprise class SDDC software to the Amazon Web Services GovCloud (US) regions, enabling customers to run any application across vSphere-based private, public, and hybrid cloud environments.

Additional Terms:

FedRAMP

Customer can view the FedRAMP Authorization status of the service at the FedRAMP Marketplace, at: https://marketplace.fedramp.gov/#!/product/vmware-government-services-vgs. If Customer requires FedRAMP authorization, Customer is responsible for reviewing the VMware Cloud on AWS GovCloud FedRAMP Package and utilizing and maintaining its configuration in a compliant manner.

DoD Data Impact Level 5 (IL5)

Customer can view the DoD Data Impact Level Authorization status of the service at the DISA Service Catalog (https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/cloud-service-support) If Customer requires DISA IL5 authorization, Customer is responsible for reviewing the VMware Cloud on AWS GovCloud Provisional Authority to Operate (P-ATO) and utilizing and maintaining its configuration in a compliant manner.

Other Accreditations

Other accreditations may be available for the service. Customer can view applicable compliance programs at https://www.vmware.com/products/trust-center.html#compliance.

Availability of Add-On Services

Core functionality of the VMware Cloud on AWS GovCloud SDDC, such as compute, storage, and networking, is equivalent to the functionality available in the commercial VMware Cloud on AWS service (i.e., VMware Cloud™ on AWS). However, some optional add-on services available in the commercial VMware Cloud on AWS service are not available, and may never be available, in the VMware Cloud on AWS GovCloud (US) service due to technical limitations and security requirements. Refer to the table below for key differences.

Add-on Service	VMware Cloud on AWS	VMware Cloud on AWS GovCloud (US)
VMware vRealize Log Insight Cloud	Available	Not Available
VMware HCX	Available	Not Available
VMware Site Recovery	Available	Available
VMware Cloud Marketplace	Available	Not Available
VMware vRealize Network Insight Cloud	Available	Not Available

Amazon Web Services Account:

Customer will not be able to access or use the VMware Cloud on AWS GovCloud (US) service without having its own AWS GovCloud (US) customer account, which Customer must establish directly with AWS. This means that if Customer does not already have an AWS GovCloud (US) account, Customer must establish one prior to being able to access the Service Offering. Prior to provisioning an SDDC, VMware requires customers to connect to their AWS account. This process establishes identity and access management policies in Customer's AWS account that enable communication between resources provisioned in Customer's AWS account and in the SDDC.

User Provisioning and Management

Unlike the VMware Cloud on AWS commercial offering (VMware Cloud™ on AWS), the VMware Cloud on AWS GovCloud (US) service requires Customer to provide its own infrastructure to manage user provisioning and authentication. As part of provisioning the VMware Cloud on AWS GovCloud (US) service, the VMware Customer Success team will work with the customer to configure user authentication against a customer-maintained Active Directory Federation Service (ADFS) server. Customers typically utilize an existing on-premises Microsoft ADFS server, or alternatively a service like AWS Directory Service (https://aws.amazon.com/directoryservice/) or Azure Active Directory Domain Services (https://azure.microsoft.com/en-us/services/active-directory-ds/) for this purpose.

Capacity Management

Customer is responsible for capacity management of its SDDCs. VMware requires that 30% unused space ("slack space") be maintained in the VMware vSAN™ datastore within the service, to support operation of the SDDC. Adequate slack space is required for use of the vSAN datastore. If storage free space reaches (or falls below) 25%, it is possible that Customer could lose the ability to utilize the SDDC, and the environment could become inoperable. If unused space in an SDDC vSAN datastore drops reaches (or falls below) 25%, VMware will automatically add hosts to the SDDC to prevent damage to the SDDC. Customer can use the VMware Cloud

sizer tool, found at https://vmcsizer.vmware.com/home, for guidance on the appropriate number of hosts needed to support anticipated workloads.

If Customer has changed the Elastic DRS for VMware Cloud™ on AWS (Elastic Distributed Resources Scheduler) ("**eDRS**") policy to "Optimize for Best Performance" or "Optimize for Lowest Cost", VMware will automatically size Customer's SDDC up or down based on load and according to the eDRS policy Customer has chosen. If Customer does not change the eDRS settings, the default option is "Scale Up for Storage Only" which means that VMware will add hosts to Customer's SDDC only when storage capacity becomes critical (that is, 25% or less free space). When eDRS is set to "Scale Up for Storage Only" VMware will not automatically scale down the SDDC.

Unless VMware and Customer otherwise agree, additional hosts added pursuant to this capacity management process will be billed at the then-current published on-demand rate for as long as those hosts are provisioned.

Data Retention and Deletion:

Customer is responsible for backing up and migrating all workloads to Customer's target environment, and deleting Customer's SDDCs, prior to termination of the Subscription Term. Customer can utilize one of multiple backup appliance vendors certified by VMware to perform workload backup and migration.

If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify VMware within five (5) days after the effective termination date, and VMware will assist Customer in extracting Customer Content from the service. Customer is responsible for all fees associated with content extraction. If Customer does not notify VMware within that 5-day period, Customer Content will be permanently deleted and will not be recoverable.

2.11 VMWARE CLOUD™ ON AWS OUTPOSTS

Overview: VMware Cloud™ on AWS Outposts delivers the VMware SDDC to a customer's location, in a fully managed service with AWS Outposts.

Amazon Web Services Account:

Customer will not be able to access or use the VMware Cloud on AWS Outposts service without having its own AWS customer account (an "**AWS account**"), which Customer must establish directly with AWS. If Customer does not already have an AWS account, Customer must establish one prior to being able to access the service. Prior to provisioning an SDDC, VMware requires customers to connect to their AWS account. This process establishes identity and access management policies in customer's AWS account that enable communication between resources provisioned in customer's AWS account and in the SDDC.

Service Location:

The service is deployed at customer premises location(s) (each, a "**Designated Facility**") specified by Customer. The fully assembled and pre-configured rack ("**system**") will be shipped to that/those location(s). An AWS technician must be provided access to the installation location(s) in a timely manner for the following activities:

- Initial site survey of the Designated Facility; this is an onsite visit by an AWS technician to validate that the Designated Facility condition and networking meet requirements for installation of the system.
- Installation of the system at the Designated Facility.
- Remediation of a problem with the service (e.g., needing to replace faulty AWS Outposts) when the issue cannot be addressed remotely.
- Retrieval of the system from the Designated Facility.

Customer must not require AWS personnel to sign, accept, or otherwise agree to any documentation as a condition of accessing the Designated Facility. Customer agrees that the terms of any such documentation are void even if signed by AWS personnel. Customer must ensure that no one accesses, moves, or repairs the AWS Outposts other than (i) personnel

designated by AWS, (ii) as permitted in writing by AWS in connection with the maintenance of the AWS Outposts, or (iii) as necessary due to a situation involving imminent injury, damage to property, or an active fire alarm system. Customer must ensure that no one modifies, alters, reverse engineers, or tampers with the AWS Outposts. Customer acknowledges that the AWS Outposts may be equipped with tamper monitoring features.

The service is linked to AWS regions. Customer selects the AWS region where the SDDC will be managed. VMware will not change the AWS region in which the SDDC is managed without Customer's prior authorization. The VMware Cloud Console data, including SDDC configuration information and data that VMware collects relating to Customer's use of the service, persists in the AWS cloud.

Customer must ensure that at all times the Designated Facility meets the minimum requirements necessary to support the installation, maintenance, use, and removal of the system, as defined here. VMware is not responsible for any delay in installation or any failure of the AWS Outposts or the SDDC if Customer does not maintain the specified environmental conditions at the Designated Facility.

Customer is not permitted to move the system from one location (premises) to another (e.g., in connection with a site consolidation), or to relocate the system within the Designated Facility premises. Any move or relocation of the system must be completed by an AWS technician. Customer must contact VMware in advance of any planned move or relocation. A fee may be charged for services to move or relocate the system.

Customer must ensure that it has all necessary rights, certifications, and licenses for the delivery, installation, maintenance, use, and removal of the system at the Designated Facility. Customer is responsible for any damage to the system while it is at the Designated Facility, unless caused by AWS.

Restriction on Modification of System:

The rack is a closed system, for use solely with the VMware Cloud on AWS Outposts service. Customer is not allowed to physically interact with or modify the system in any way, nor to modify the service software except as expressly permitted. All interactions with the service must be through the VMware Cloud Console, except the vCenter Service Appliance, which can be accessed through the service console, or from within Customer's SDDC through the uplink connection.

When Customer receives the system at the Designated Facility, Customer must not open or disturb the package containing the system, and must keep the package in a safe location at the Designated Facility until an AWS technician arrives to unbox the system, set it up, configure it, and power it on. Thereafter, any problems with the system will be handled through the support process.

If Customer directly accesses (except through direct vCenter access) or modifies the system any way, it may result in relieving VMware of its support obligations, and VMware may choose to discontinue the service at the compromised location, and/or terminate Customer's entitlement to the service.

Service Offering Hardware:

Title to the AWS Outposts remains at all times in AWS, and Customer acquires no right or interest in the AWS Outposts by virtue of ordering a subscription to the service. VMware reserves the right to replace the AWS Outposts (with the assistance of AWS) at Customer's location(s) at any time for any reason.

At VMware's discretion, AWS Outposts may be refreshed by AWS at the end of a customer's committed subscription term, depending on the length of the original subscription term and any renewal term. AWS Outposts will not be refreshed during a committed subscription term. In the event of an AWS Outposts refresh, VMware will assist Customer in migrating data and workloads to the new AWS Outposts.

Data Retention and Deletion:

If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer has 45 days after termination of the Subscription Term within which to notify VMware that Customer wishes to extract Customer Content and to complete that extraction, before an AWS technician removes the system from the Designated Facility. If Customer requests, VMware will assist Customer in

extracting Customer Content. Customer is responsible for all fees associated with content extraction. If Customer does not notify VMware before the system is removed from the Designated Facility, Customer Content will be permanently deleted and will not be recoverable.

2.12 VMWARE CLOUD™ ON DELL

Overview: VMware Cloud™ on Dell is a VMware-managed cloud service that brings VMware's enterprise class SDDC software on Dell hardware to a customer's on-premises environment.

Cloud Service Location:

VMware Cloud on Dell is deployed at the street address location(s) that Customer specified when ordering the service. The fully assembled and pre-configured rack ("**system**") will be shipped to that/those location(s).

NOTE: The VMware Cloud on Dell service may not be available for deployment in all geographies. Customer must verify the service's availability at Customer's selected installation location.

Customer must allow a Dell-authorized technician access to the installation location(s) in a timely manner for the following activities:

- Initial site survey – In most cases, initial site survey information is collected through the VMware Cloud Console during the ordering process. In some cases, Customer may be contacted to verify certain information. For complex deployments, an engineer may need to visit the installation site for an on-site survey.
- Installation of the system and activation of the service.
- Remediation of a problem with the service (e.g., needing to replace faulty hardware) where the issue cannot be addressed remotely.
- Retrieval of the system from Customer's installation site(s).

Any delays in providing access to the installation site(s) will affect the response times(s) VMware provides for any required on-site activities.

Each installation site must comply with the published environmental specifications for the service (e.g., temperature, humidity, power, etc.). VMware is not responsible for any delay in installation or any failure of the hardware or the SDDC if Customer does not maintain the specified environmental conditions at the installation site(s). See https://docs.vmware.com/en/VMware-Cloud-on-Dell-EMC/index.html for the environmental specifications.

Customer is not permitted to move the system from one location (premises) to another (e.g., in connection with a site consolidation), or to relocate the system within Customer's premises. Any move or relocation of the system must be done by a Dell or a Dell-authorized technician. Customer must contact VMware in advance of any planned move or relocation. A fee may be charged for services to move or relocate the system.

The VMware Cloud Console data, including Customer's SDDC configuration information and data that VMware collects relating to use of the VMware Cloud on Dell service, persists in VMware owned, managed, and controlled data repositories in the AWS cloud.

VMware is the single point of contact for all support requests for the VMware Cloud on Dell service. Hardware break-fix support will be performed by Dell or Dell's approved third-party partners for specific infrastructure elements like UPS, PDU, etc., upon request from VMware.

Full availability of the VMware Cloud on Dell service is dependent upon and subject to the performance of the Dell hardware components, and of the AWS infrastructure on which the VMware Cloud Console is hosted.

Cloud Service Hardware:

Title to the VMware Cloud on Dell service hardware ("**Hardware**") remains in Dell at all times. Dell retains all right, title, and interest in and to the Hardware at all times, and Customer acquires no right or interest in the Hardware by virtue of ordering a subscription to the VMware Cloud on Dell service.

VMware reserves the right to replace the Hardware (with the assistance of Dell or a Dell-authorized technician) at Customer's location(s) at any time for any reason, consistent with the agreement between VMware and Dell. VMware also reserves the right to reuse the Hardware for different customers when appropriate. If VMware elects to provide previously deployed Hardware to Customer, the Hardware that is delivered will have all previous data and configurations completely deleted.

At VMware's discretion and consistent with the agreement between VMware and Dell, the Hardware may be refreshed by Dell or a Dell-authorized technician at the end of Customer's committed subscription term, depending on the length of the original subscription term and any renewal term. Hardware will not be refreshed during a committed subscription term. In the event of a Hardware refresh, VMware will assist Customer in migrating data and workloads to the new Hardware.

The Hardware is a closed system, for use solely with the VMware Cloud on Dell service. Customer is not allowed to physically interact with or modify the Hardware in any way, nor to modify the VMware Cloud on Dell service software except as expressly permitted. All interactions with the VMware Cloud on Dell service must be through the VMware Cloud Console, except the vCenter Service Appliance, which can be accessed through the VMware Cloud on Dell service console, or from within Customer's SDDC through the uplink connection.

When Customer receives the system at Customer's premises, Customer must not open or disturb the package containing the system, and must keep the package in a safe location at the premises until a Dell-authorized technician arrives to unbox the system, set it up, configure it, and power it on. Thereafter, any problems with the system will be handled through the support process.

If Customer directly accesses (except through direct vCenter access) or modifies the system any way, it may result in relieving VMware of its support obligations, and VMware may choose to discontinue the VMware Cloud on Dell service at the compromised location, and/or terminate Customer's subscription.

Data Retention and Deletion:

Retention and storage policies associated with Customer Content (including any personal data stored within Customer Content) for the VMware Cloud on Dell service are solely managed by Customer. VMware does not back up Customer Content and therefore will not be able to recover any Customer Content in any unforeseen event. Customer is responsible for implementing tools, products, and operational procedures to support data migration, data protection, backup/archive, and restoration for all Customer Content and all configurations created by Customer in the SDDC, including virtual machines and content libraries.

At the end of the Subscription Term, Customer has 45 days from the time VMware notifies Customer within which to delete Customer Content from the system. If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so), Customer must notify VMware before a Dell-authorized technician removes the Hardware from Customer's premises, and VMware will assist Customer in extracting Customer Content from the service. Customer is responsible for all fees associated with extracting Customer Content. If Customer does not notify VMware before system removal, a Dell-authorized technician will remove the system from Customer's premises. If Customer has not deleted Customer Content from the system, it will be deleted by Dell.

2.13 VMWARE EDGE NETWORK INTELLIGENCE™

Overview: VMware Edge Network Intelligence™ is a SaaS-based Artificial Intelligence for IT Operations (AIOps) solution that provides proactive actionable intelligence to ensure that end-user and IoT devices at the edge of distributed and secure enterprise networks get the performance and analytics they need from WLAN, LAN, WAN, and SASE network services and applications to which they connect. VMware Edge Network Intelligence employs machine learning algorithms and modern big data analytics to process high volumes of data from a wide range of networks, devices, and applications. In doing so, the service auto-discovers end-user and IoT devices, automatically establishes baselines, understands client interactions, and monitors for deviations to provide actionable insights that operations teams can proactively remediate.

VMware Edge Network Intelligence analytics edge software ("**Software**") is installed on edge devices provided by VMware (each, a "**Device**") or on other equipment ("**Equipment**") at Customer's location. (As used in this Section 2.13, any Device or Equipment with the Software installed is an "**Edge**".) The Software collects performance metrics from across the network stack and examines network traffic by performing deep packet inspection. The extracted performance metrics are sent to the service platform for analysis.

Additional Terms:

Notwithstanding the provisions in the General Terms, the Cloud Exhibit, and Customer's Order, the Subscription Term will begin on the first to occur of (i) the date Customer's instance of the VMware Edge Network Intelligence service has been provisioned or (ii) the end of Customer's deployment window if a deployment window was quoted and ordered. The Subscription Term may begin prior to installation of the Edge in Customer's designated location. VMware may permit Customer to continue to use the VMware Edge Network Intelligence service for an additional period, not to exceed 30 days, after expiration of the committed Subscription Term, at no additional cost, if the Subscription Term began prior to installation of the Edge. All terms, other than payment of fees, will continue to apply during any extended use term.

Data Retention and Deletion:

During the Subscription Term, Customer Content transmitted to VMware Edge Network Intelligence will be retained and available for querying and alerts for approximately two weeks from the date and time the data point was originally ingested into the service, after which time it is deleted. During the Subscription Term, any log files containing Customer Content will be deleted approximately 30 days after their creation.

Termination of the Subscription Term will result in deletion of all Edge configuration and data. Customer Content will be deleted within approximately 14 days after the termination date. Any log files containing Customer Content will be deleted approximately 30 days after the termination date. During this 14-day period, data will not be generally accessible. Any deleted data is non-recoverable.

2.14 VMWARE HCX®

Overview: VMware HCX® enables IT organizations to securely connect their VMware infrastructure across both public and private data centers for hybrid capabilities such as workload migration and disaster recovery. VMware HCX can be consumed via a user interface (UI) or an application programming interface (API), at either the source or the destination environment. Certain operations are context-aware and may only be available at the source environment but not the destination environment, or vice versa.

Data Retention and Deletion:

VMware HCX provides the ability to back up the service's configurations, including deployment settings such as network information, to enable a successful recovery if the environment becomes corrupted or lost through an event such as hardware failure; this is Customer's responsibility to configure. If Customer's entitlement is out of support or is disconnected from the VMware HCX service for greater than 90 days, the entitlement will be terminated. Termination of an entitlement will result in permanent loss of access to the environments, discontinuation of services, and a deletion of such environments, configurations, and data according to applicable VMware policies. VMware retains hashed, anonymized data in its systems. Customer data related to metered usage will be stored in the VMware analytics cloud and may be kept longer than 90 days.

2.15 VMWARE HORIZON® SERVICE

Overview: VMware Horizon® Service includes two individual services: VMware Horizon® subscription, and VMware Horizon® Cloud Service™ on Microsoft Azure.

- Horizon subscription delivers virtual desktops and applications on VMware SDDC-based infrastructure (whether in Customer's on-premises environment or in a hosted environment) and connects to the Horizon Cloud control plane through the VMware Horizon® Cloud Connector™.
- Horizon Cloud Service on Microsoft Azure delivers cloud-hosted virtualized desktops and applications from a customer's own Microsoft Azure infrastructure capacity. Customers pair their Microsoft Azure infrastructure capacity with the Horizon Cloud Service.

If Customer's Horizon Service entitlement includes VMware vSphere® Desktop, VMware vCenter®, and VMware vSAN™ Advanced for Desktop, Customer's use of those products is limited to managing Horizon workloads: specifically, Desktop Virtual Machines, Terminal Services Sessions, remote desktop services that host and run VMware products which are included in the VMware Horizon bundle, or third party connection brokers and desktop management and monitoring tools.

As stated in the Product Guide, if Customer receives its entitlement to the Horizon Service under the VMware Subscription Upgrade Program for Horizon, Customer agrees to relinquish its entitlements to any corresponding Horizon on-premises perpetual licenses, and complete its migration to the Horizon Service, within 90 days after the effective date of the relevant agreement (e.g., an Enterprise License Agreement ("**ELA**"), or an amendment to an ELA, etc.). Customer's failure to complete that migration within 90 days will result in VMware ceasing support of Customer's on-premises Horizon environment, and Customer will have no further access to upgrade and installer files. After Customer has completed the migration to the Horizon Service, Customer must not use any license keys related to the on-premises perpetual licenses, and VMware will invalidate those keys. Customer is not required to uninstall any Software if Customer converts its existing Horizon on-premises perpetual licenses deployment to Horizon Service entitlements by installing the Horizon Cloud Connector and managing licenses through the Horizon Cloud control plane, which must be done within 90 days after purchase of Customer's entitlement, as provided above in this Section 2.15.

VMware Workspace ONE® Access™:

VMware Horizon Service includes VMware Workspace ONE® Access™, hosted by VMware. Use of Workspace ONE Access within the Horizon Service requires a Workspace ONE Access connector, which can be installed and managed on a customer's virtual machine or on a utility server.

VMware Advanced Monitoring powered by ControlUp - Optional Add-On:

VMware Advanced Monitoring powered by ControlUp is a third-party solution that delivers a real-time monitoring and visualization engine for VMware Horizon that allows customers to have a unified console for monitoring, triggers and alerts, troubleshooting, and automation for their Horizon deployment. VMware Advanced Monitoring allows customers to monitor their entire VMware Horizon environment, detect anomalies, and proactively solve issues across their deployment. VMware Advanced Monitoring has an analytics engine that provides insights and reporting on the data that is collected from a customer's environment. VMware Advanced Monitoring is hosted by ControlUp, Inc., from its data centers. Customer must purchase an equivalent number of seats for VMware Advanced Monitoring as purchased for the Horizon Service.

VMware will provide support for the Advanced Monitoring offering. The General Terms and the Cloud Exhibit govern Customer's use of VMware Advanced Monitoring and will supersede any terms presented to Customer during the deployment and sign-in process for VMware Advanced Monitoring. If Customer uses the Advanced Monitoring service in an on-premises environment, then the General Terms and the Software Exhibit will govern that use. Notwithstanding anything in the General Terms, the Cloud Exhibit, and/or the Software Exhibit, and other than as expressly set forth in this Section 2.15, VMware provides the VMware Advanced Monitoring service without any indemnification or warranty whatsoever.

2.16 VMWARE LAB PLATFORM™

Overview: VMware Lab Platform™ (formerly known as VMware Learning Platform™) is a cloud service that provides the mechanism to deliver true hands-on education content to anyone, worldwide, at cloud scale. It allows Customer to train on anything that can be installed on an operating system. Customers can access the Service Offering from any device that has a web browser with no plug-ins needed and nothing additional to install.

Google Analytics: VMware Lab Platform utilizes Google Analytics

Data Retention and Deletion:

During the Subscription Term, data transmitted to VMware Lab Platform by Customer will be retained and available for querying and alerts. Upon expiration of the Subscription Term, all data will be deleted.

2.17 VMWARE NSX® ADVANCED LOAD BALANCER™

Overview: VMware NSX® Advanced Load Balancer™ provides multi-cloud load balancing, web application firewall, application analytics, and container ingress services from the data center to the cloud with enhanced operations delivered as a software as a service offering. NSX Advanced Load Balancer can be deployed in a customer's own on-premises environment and/or consumed as a hosted service.

Additional Terms:

Customer may use NSX Advanced Load Balancer cloud service entitlements with earlier versions of the on-premises version of NSX Advanced Load Balancer, provided that Customer's total deployment does not exceed what Customer has purchased. If Customer requests, VMware will provide Customer with license keys that may be used with those earlier versions of the on-premises version of NSX Advanced Load Balancer. The license keys will not unlock any features or functionality that are only available in later versions of the offering. To use NSX Advanced Load Balancer cloud service entitlements with the on-premises version of NSX Advanced Load Balancer, the on-premises software version must be 21.1.3 or higher.

Subscription Upgrade Program:

If Customer receives its entitlement to NSX Advanced Load Balancer through the Subscription Upgrade Program for NSX Advanced Load Balancer, Customer agrees to relinquish its entitlements to any corresponding NSX Advanced Load Balancer on-premises perpetual licenses (the "**Software**"), and to complete migration to the cloud service, within 90 days after the effective date of the relevant agreement pursuant to which Customer purchased its entitlement to the service (e.g., an Enterprise License Agreement ("**ELA**"), or an amendment to an ELA, etc.). Failure to complete this migration within 90 days will result in VMware ceasing support of Customer's on-premises NSX Advanced Load Balancer environment, and Customer will have no further access to upgrade and installer files. After Customer has completed its migration to the hosted service, Customer must not use any license keys related to the on-premises perpetual licenses, and VMware will invalidate those keys. Customer is not required to uninstall any Software if Customer converts its existing NSX Advanced Load Balancer on-premises perpetual licenses deployment to the NSX Advanced Load Balancer service by registering the NSX Advanced Load Balancer deployment with NSX Advanced Load Balancer, and managing licenses through the central licensing service provided by NSX Advanced Load Balancer cloud services, which must be done within 90 days after purchase of Customer's entitlement, as provided above in this Section 2.17.

Data Retention and Deletion:

During the Subscription Term, content will be backed up every day and stored encrypted with the retention policy of one daily backup for the most recent 60 days. VMware will make Customer Content available for export for a period of 60 days following the effective Subscription Term termination date. If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify VMware within thirty (30) days after the effective termination date, and VMware will assist Customer in extracting Customer Content from the service. Customer is responsible for all fees associated with content extraction.

2.18 VMWARE NSX DEFENDER, VMWARE NSX DETONATOR

[Reserved]

2.19 VMWARE PIVOTAL TRACKER

Overview: Pivotal Tracker® Enterprise SaaS is an agile project management and collaboration tool that enables users to track anticipated delivery of action items based on the team's performance.

A Quick Start guide, workflow guides for navigating through key features, and full product help and documentation are available in the Tracker Help Center. Public documentation that explains how to get started with the API (Application Programming Interface) and examples for various API calls is provided in the API documentation.

Definitions: For purposes of this Section 2.19, the following terms have the following meanings:

"Account" means a group of Projects associated with a payment plan. Accounts have one Account Owner, and can have as many Projects and Project Members as the plan for the particular Account allows.

"Account Owner" is the individual or Organization representative responsible for the payment and billing for a particular Account.

"Project" means a space to organize and collaborate around information in the form of user stories, with controlled access to specific individuals or the public (for read-only access), based on Project access settings.

"Project Member" means a specific person, identified by a User ID, who has been explicitly invited to a Project.

"User ID" means the email and username by which a person identifies their User Profile

"User Profile" means the information a user provides, including username, full name, email, and other Login Credentials.

Google Analytics: Pivotal Tracker utilizes Google Analytics.

Evaluation/Trial:

VMware offers a free of charge trial of Pivotal Tracker for customers that want to evaluate the service prior to deciding whether or not to purchase a paid subscription. During the trial, Customer may associate an unlimited number of Projects and Project Members with its Account, and the Account will have access to the full functionality of Pivotal Tracker. A credit card is not required for the trial. At the end of the trial, if Customer does not upgrade to a paid plan, the Account will transition to the free plan as described on the service's "Plans and Billing" page. If Customer's Account exceeds the limits associated with the free plan, the Account will be suspended, and all Projects in the Account will become read-only until the Account is either (a) brought below the free plan limits or (b) Customer purchases a paid subscription for a plan for which the Account qualifies. Customer may upgrade an Account to a paid plan prior to the

expiration of the trial, and VMware will not charge Customer until after the trial except as set forth on the Plans and Billing page.

Only the first Account that Customer creates will be eligible for the trial. Additional Accounts that Customer creates will start on the free plan, as published on the Plans and Billing page. Customer may not move Projects in or out of Accounts that are in the trial. Customer is entitled to only one trial. Only one organization representative is entitled to receive the trial.

Data Retention and Deletion:

During the Subscription Term, Accounts, Projects, individual stories, and attachments to those stories can all be deleted at any time by users with the correct permissions. Any additional data access/deletion requests can be made by contacting support@pivotaltracker.com or privacy@vmware.com. The service's data deletion policy is described publicly here,

If any Customer Content is deleted during the Subscription Term, that data will be deleted from VMware's primary database within 24 hours, and from back-up databases, if applicable, within seven days.

Following expiration of the Subscription Term, VMware will retain Customer Content for 30 days, following which period it will be deleted. Customer will not have any access to Customer Content during that 30-day period.

2.20 VMWARE REMOTEHELP™

Overview: VMware RemoteHelp™ provides a standalone platform for carrier customer care technicians and IT admins within MSPs/OEMs to remotely diagnose, support, and troubleshoot problems on end users' mobile devices.

Data Retention and Deletion:

During the Subscription Term, all data older than 90 days is purged on a scheduled job. Following termination of Customer's entitlement, all Customer Content will be deleted within 30 days after the effective termination date.

2.21 VMWARE SASE™

Overview: VMware SASE™ is a cloud-native secure access service edge platform that combines VMware SD-WAN™, VMware Secure Access™, VMware Cloud Web Security™, and VMware Enterprise Network Intelligence™ into one holistic solution. The platform's points of presence (PoPs) are strategically distributed around the world and serve as an on-ramp to SaaS and other cloud services.

VMware SD-WAN

VMware SD-WAN™ is a cloud-delivered software-defined wide area network (SD-WAN) service that provides networking services to enterprise branch locations, and to customers' remote location workers through the "work from home" offer described below.

VMware Secure Access

VMware Secure Access™ is a remote access solution that is based on Zero Trust Network Access (ZTNA) framework.

VMware Cloud Web Security

VMware Cloud Web Security™ is available as an add-on to VMware Secure Access or to VMware SD-WAN. Customer must have an active subscription to the VMware SD-WAN service or to VMware Secure Access to purchase an entitlement to VMware Cloud Web Security.

VMware SD-WAN Work from Home Offer

Enterprise customers that have employees working from home can purchase SD-WAN subscriptions to support their remote workforce, through the VMware SD-WAN™ WFH Subscription ("**WFH Subscription**") and the VMware SD-WAN™ WFH Pro Subscription ("**WFH Pro Subscription**") offer.

Subscriptions purchased through this offer can only be used at employees' home locations. For the WFH Subscription there is a limit of one business user with two concurrent devices and up to 350 Mbps or the max throughput of the Edge (whichever is lower). For the WFH Pro Subscription there is a limit of one business user with three concurrent devices and up to 1 Gbps or the max throughput of the Edge (whichever is lower). Both the WFH Subscription and the WFH Pro Subscription offers allow for an unlimited number of home users and devices. The key difference between a business user and home user is that the business user can send traffic to the gateways, to other SD-WAN Edges, or directly to the Internet, but the home user can only send traffic directly to the Internet. Business users and home users must use separate network segments. Both WFH Subscription and WFH Pro Subscription subscriptions will provide access to the same feature set as VMware SD-WAN.

For purposes of this Section 2.21 and this work from home offer, a "**business user**" means an individual who is the customer's designated User (e.g., an employee of Customer, an independent contractor performing services for Customer, or a person who is otherwise one of Customer's designated Users). A "**home user**" means an individual who is not a "business user" or who is not acting as a "business user" but is connected to the VMware Edge in the business user's home, by WiFi or physical port. A "home user" may also be a "business user" of the customer (i.e., a "business user" acts as a "home user" when (s)he is using a personal device (e.g., personal laptop, personal mobile device, gaming system, smart TV, etc.).

VMware reserves the right to audit customers by checking the Edge logs to verify adherence to the requirements of this work from home offer.

VMware reserves the right to terminate this work from home offer at any time. However, termination of the offer will not operate to terminate SD-WAN WFH Subscriptions or WFH Pro Subscriptions purchased pursuant to the offer; those subscriptions will expire according to their terms, but cannot be renewed.

Additional Terms:

In connection with Customer's order for any of the SASE offerings, Customer will need to provide information such as site count, site location(s), feature(s), throughput(s), and Customer's network administrator's email. The information Customer provides is required to provision the service. Notwithstanding anything to the contrary in the General Terms, the Cloud Exhibit, or the Order, the Subscription Term will begin on the date Customer's instance of the service has been provisioned. If Customer does not provide the needed information, VMware cannot provision the service.

For SD-WAN subscription purchases including Equipment, the Subscription Term may begin prior to installation of the Equipment in Customer's location. VMware may permit Customer to continue to use the service for an additional period, not to exceed 30 days, after expiration of the committed Subscription Term, at no additional cost, if the Subscription Term began prior to installation of the Equipment. All terms, other than payment of fees, will continue to apply during any extended use term.

VMware SD-WAN edge software ("**Software**") is installed on customer-premises equipment ("**Equipment**") at the Customer location (that is, in Customer's own on-premises environment). The Equipment can be supplied by VMware, or by Customer (provided that the equipment supplied by the customer is x86 compatible). The Software and the Equipment are referred to collectively as the Edge for VMware SD-WAN (the "**Edge**"). The VMware SD-WAN orchestrator ("**Orchestrator**") is a solution that provides centralized enterprise-wide installation, configuration, and real-time monitoring in addition to orchestrating the data flow through the cloud network. The Orchestrator enables remote provisioning of virtual services in Customer's location, in the public cloud, or in Customer's enterprise data center. This centralized management portal provides insight into global network operation, as well as serving as a central policy engine that supplies the Edge with both network intelligence as well as administrative policies on how applications behave in the enterprise SD-WAN network. The Orchestrator is hosted and managed by VMware. The service also provides access to a global, distributed set of VMware cloud gateways ("**Gateway(s)**"), that serve as a distributed forwarding plane, and are responsible for delivering network traffic to its final destination. In the process of transport, reliability and performance enhancements are applied to the carried traffic that improve the end-user

application experience at the enterprise locations. Gateways are hosted and managed by VMware.

Data Retention and Deletion:

VMware SD-WAN: As VMware SD-WAN is used, the Edges and Gateways send data to the Orchestrator including flow statistics (Edge ID, hostname, source and destination IP address, source MAC address, throughput, destination domain name, protocol, application. and application category) and link statistics (ISP name, Public IP address, bandwidth, speed, latency, packet loss and jitter). During the Subscription Term, data transmitted to VMware SD-WAN will be retained in the Orchestrator and available for querying and alerts for at least two weeks (by default) from the date and time the data was originally ingested into VMware SD-WAN. The amount of data stored depends on the storage space available on the Orchestrator and the amount of data generated by each site's Edge.

VMware Secure Access: VMware Secure Access processes identity and authentication information, device information, communication data, geo-location data, and application access/usage details. This data is not retained after it is processed.

VMware Cloud Web Security: Depending on Customer's configuration of VMware Cloud Web Security, workload data selected by Customer is sent to VMware Cloud Web Security for security checks as designated by Customer. Customer may define which workloads pass through which security checks based on criteria including network-based filters such as subnet and IP address, and non-network-based filters such as users, groups, file type, application, and domain.

2.23 VMWARE TANZU™ MISSION CONTROL™

Overview: VMware Tanzu™ Mission Control™ is a centralized management platform for consistently operating and securing a customer's Kubernetes infrastructure and modern applications across multiple teams and clouds. VMware also offers the VMware Tanzu® Mission Control™ Starter edition (the "**Starter Service**"), described below. References in this Section 2.23 to the "service" apply to both VMware Tanzu Mission Control and to the Starter Service, except as expressly provided.

VMware Tanzu Mission Control can be purchased as a standalone service or as part of a Tanzu Edition software bundle. Any on-premises components, for example those included in Tanzu Standard, are subject to the General Terms, the Software Exhibit, and the Product Guide. If an entitlement to Tanzu Mission Control is purchased as part of a Tanzu edition, please refer to the Product Guide.

Tanzu Mission Control Starter Service:

VMware Tanzu Mission Control Starter ("**Starter Service**") is a defeatured, consumption-limited, free (no charge) version of Tanzu Mission Control. Customer gets access to a subset of the features of the Tanzu Mission Control service. There is no time limit on Customer's use of the Starter Service. VMware does not provide any support for the Starter Service, nor does the Tanzu Mission Control Service Level Agreement apply to the Starter Service. The Starter Service should not be used in any environment that requires production level service level guarantees or support.

Customer can upgrade from the Starter Service to the standard service by purchasing an entitlement to Tanzu Mission Control as a standalone service or as part of a Tanzu Edition software bundle.

Starter Service users are entitled to a limited amount of Tanzu Mission Control: 5 clusters and 100 vCPUs (as of the date of this Services Guide). VMware reserves the right to change the amount of Tanzu Mission Control a Starter Service user can consume, and the features of Tanzu Mission Control that are accessible through the Starter Service; VMware will give Customer reasonable prior notice of any change. Customer can monitor the amount of the Starter Service that it is consuming through the Administration > Subscription information page in the Tanzu Mission Control console. The Starter Service is architected so that a user cannot consume more of Tanzu Mission Control than its entitlement allows. Organization administrators will receive an email notification when the organization is close to reaching the Starter Service limits. If Customer needs more Tanzu Mission Control capacity than the Starter Service provides, Customer must purchase a subscription to the Tanzu Mission Control service. If a Starter Service user has been

inactive for 60 days, the account will be considered closed. All account information will be deleted 90 days after the account is considered closed, and the account will be considered terminated.

Data Retention and Deletion:

VMware will retain Customer Content in VMware's active data stores for 90 days following the effective termination date of the Subscription Term. After this 90 day period, all Customer Content is deleted from VMware's active data stores. Backups of VMware's active data stores that may contain Customer Content will be overwritten and destroyed within 35 days of Customer Content being deleted from VMware's active databases. If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify VMware within 10 days after the effective termination date, and Customer must be able to complete extraction of Customer Content within the 90 day post-termination period. VMware will assist Customer in extracting Customer Content from the service. Customer is responsible for all fees associated with extracting Customer Content. If Customer does not notify VMware within 10 days after the effective termination date, Customer Content will be permanently deleted and will not be recoverable after the 90 day post-termination period.

2.24 VMWARE TANZU™ OBSERVABILITY™ BY WAVEFRONT

Overview: VMware Tanzu™ Observability™ by Wavefront is a SaaS-based observability platform that handles the high-scale requirements of modern cloud-native applications. Tanzu Observability ingests a variety of data sources that are processed and stored as time-series telemetry, that can be analyzed, visualized, and alerted upon for optimization, status reporting, anomaly detection, and troubleshooting of modern cloud applications.

Additional Terms:

When Customer orders a subscription to the service, Customer will be required to fill out a provisioning questionnaire provided by VMware (via email or a link to the online account configuration portal). The information Customer provides is required to provision the service. It is Customer's responsibility to complete and return the questionnaire within ten (10) business days after submitting the Order. The Subscription Term will begin on the date the service has been provisioned. If Customer does not provide a completed questionnaire, VMware will provision Customer's instance of the service on a commercially reasonable basis.

Software provided at https://github.com/wavefronthq ("**Enabling Software**") is available to use or send data to the service. The Enabling Software is provided under applicable open source licensing terms as indicated in the source code repository. Customer is responsible for obtaining, installing, and maintaining the Enabling Software. VMware makes no representations or warranties, nor is otherwise liable or obligated pursuant to the Agreement, with respect to the Enabling Software. VMware will not provide support with respect to the Enabling Software.

Data Retention and Deletion:

During the Subscription Term, Customer Content submitted to the service will be retained and available for querying and alerts, and is retained for 19 months from the date and time the data was originally submitted to the Service Offering.

Following expiration or termination of the Subscription Term, all Customer Content, and all personal data contained in Customer Content will be deleted from VMware's systems within the following time frames: 18 months for Metrics, 6 months for Distributions, and 7 days for Traces.

2.25 VMWARE TANZU™ SERVICE MESH ADVANCED EDITION

Overview: VMware Tanzu™ Service Mesh™ Advanced edition provides a platform-neutral, application-level networking and security stack, to increase application visibility, security, and

resiliency for highly-distributed cloud-native applications. Tanzu Service Mesh Advanced allows customers to gain insights into applications regarding users, microservices, and data sources running across a variety of heterogeneous infrastructures, by collecting and consolidating performance, health, and security metrics. This creates a single network and security operations management plane across those infrastructures, through which the customer can connect, secure, and troubleshoot cloud-native applications. Customers can access the service through a web browser and by using scripts/code through a public API.

Microservices can discover and route traffic to other microservices and data sources through a platform-neutral distributed service catalog provided by Tanzu Services Mesh Advanced. Since each microservice has a secure identity provided by the service, microservices can also authenticate and encrypt their communications with no changes to application code.

Tanzu Service Mesh Advanced also provides an intent-based policy engine that customers can use to specify the desired traffic management, service level objectives, and security requirements for their applications. Policies can use dynamic contextual information collected either from the platforms where the microservices are running, or from integrations with other third-party products.

Data Retention and Deletion:

During the Subscription Term, data transmitted to the service by Customer will be retained and available for querying and alerts. Data is retained for a period not to exceed 12 months from the date and time the data was originally ingested into the service.

VMware will retain Customer Content in its backup systems for 30 days following the effective termination date of the Subscription Term. If Customer wishes to extract Customer Content from the service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify VMware within ten (10) days after the effective termination date, and VMware will assist Customer in extracting Customer Content from the service. Customer is responsible for all fees associated with content extraction. If Customer does not notify VMware within that 10-day period, Customer Content will be permanently deleted and will not be recoverable.

2.26 VMWARE vCLOUD® USAGE INSIGHT™

[Service deprecated; partners migrated to Cloud Partner Network]

2.27 VMWARE vREALIZE® AUTOMATION CLOUD™

Overview: VMware vRealize® Automation Cloud™ consists of the following component services: VMware Cloud Assembly™, VMware Code Stream™, and VMware Service Broker™

VMware Cloud Assembly™ ("**Cloud Assembly**") is a cloud automation service purpose-built for provisioning and managing workloads in SDDCs, VMware Cloud™ on AWS–based clouds, and public clouds. Cloud Assembly offers powerful infrastructure-as-code capabilities to build, deploy, and iterate on applications with agile governance.

VMware Code Stream™ ("**Code Stream**") is an application release automation offering that helps customers automate their Continuous Integration and Continuous Delivery processes. Code Stream focuses on ease of release pipeline modeling, deep integration with other VMware services, such as Cloud Assembly, and non-VMware products, such as source code control systems, and enhanced reporting through dashboards to help DevOps teams with deep visibility and automation of the software release process.

VMware Service Broker™ ("**Service Broker**") is a storefront for self-service consumption of ready-to-use templates and services with guardrails. This collection of ready-to-consume cloud services and templates is aggregated from multiple cloud platforms and providers.

The resources or catalog items deployed and managed by vRealize Automation Cloud are provisioned on private and public cloud platforms pre-configured by Customer. There may be additional charges associated with consuming public cloud services billed to Customer

separately by its providers. Activities such as sending logs over the internet and building code on Customer's public cloud environments may incur additional compute and network usage charges billed to Customer by its providers.

Use of FullStory:

Hosted components of vRealize Automation Cloud use FullStory functionality to collect data directly from any browsers used to access and use the service. FullStory collects data regarding a person's use of the service, including user interaction and behavior, to enable session replay. The data collected and inferred is used by VMware to diagnose and improve its products and services, and to address issues. For users who wish to opt out of session recording, FullStory makes the following website available: https://www.fullstory.com/optout/. Customer agrees to provide the information, above, regarding Usage Data and FullStory usage to all Users of the service.

VMware vRealize® Automation SaltStack® SecOps – Optional Add-On:

The hosted version of VMware vRealize® Automation SaltStack® SecOps (also referred to as "**SaltStack SecOps Cloud**") is a SaaS-based compliance and vulnerability management application that can automate security remediation. It is sold as a separate add-on subscription. To use the SaltStack SecOps Cloud add-on, Customer must have an active subscription to vRealize Automation Cloud or to another offering that contains the service (e.g., VMware vRealize® Cloud Universal™). Customer does not have to purchase the same quantity of the SaltStack SecOps Cloud add-on as the quantity of the vRealize Automation Cloud service that Customer has purchased, but Customer may only deploy the add-on in the same environment where vRealize Automation Cloud is deployed.

If Customer has purchased a license to the on-premises perpetual version of VMware vRealize Automation SaltStack SecOps, Customer may take advantage of VMware's Subscription Upgrade Program (SUP) to upgrade that license to SaltStack SecOps Cloud by purchasing the appropriate upgrade entitlement. If Customer receives its entitlement to SaltStack SecOps Cloud through the SUP, Customer agrees to relinquish its entitlements to the relevant on-premises perpetual licenses within 30 days after the purchase of the subscription to the SaltStack SecOps Cloud add-on. Not later than 30 days after Customer's purchase of the SaltStack SecOps Cloud add-on, Customer must stop using any license keys related to the on-premises perpetual software product, and VMware will invalidate these license keys; thereafter, Customer will not be able to use the on-premises product.

The SaltStack SecOps Cloud add-on is offered for committed subscription terms; that is, it cannot be consumed on an on-demand basis. If Customer's subscription to vRealize Automation Cloud is terminated while the add-on subscription is still active, Customer will not be able to use the add-on. Customer will not be entitled to any refund for the remaining portion of the add-on subscription term.

VMware vRealize® Automation Cloud Guardrails™ - Optional Add-On:

VMware vRealize® Automation Cloud Guardrails™ provides an infrastructure-as-code solution for users to set up and manage policies for configuration, security, networks, performance, availability, and cost of their multi-cloud environment. As of the date of this Services Guide, vRealize Automation Cloud Guardrails is free of charge; VMware anticipates charging customers for use of this feature in the future. Customers will be notified by VMware when the free offer of the vRealize Automation Cloud Guardrails ends. At that time, customers will be able to upgrade use of this feature by purchasing a paid subscription.

2.28 VMWARE vREALIZE® CLOUD UNIVERSAL™

Overview: VMware vRealize® Cloud Universal™ is a cloud management suite that includes on-premises and hosted components. vRealize Cloud Universal is the successor offering to VMware vRealize® Cloud™ and VMware vRealize® Flex™.

VMware Cloud Upgrade Program:

If Customer receives its entitlement to vRealize Cloud Universal through the VMware Cloud Upgrade Program, then within 30 days of the purchase of the entitlement, Customer agrees to relinquish its entitlements to relevant on-premises perpetual licenses for vRealize Suite, vRealize Operations, vRealize Automation, vRealize Log Insight, or vSphere Enterprise Plus that were exchanged through the vRealize Cloud Universal Subscription Upgrade Program ("**Exchanged Licenses**"). Customer must stop using any license keys related to the Exchanged Licenses, and VMware will invalidate the license keys for the Exchanged Licenses. Customer is not required to uninstall any Software if Customer converts its existing on-premises perpetual licenses to a vRealize Cloud Universal entitlement by applying vRealize Cloud Universal license key to Customer's existing Software instances, using vRealize Suite Lifecycle Manager.

2.29 VMWARE vREALIZE® LOG INSIGHT CLOUD™

Overview: VMware vRealize® Log Insight Cloud™ is a log-based monitoring and troubleshooting service, purpose-built for SDDCs, both in a customer's on-premises environment as well as on VMware Cloud™ on AWS, and for public clouds.

2.30 VMWARE vREALIZE® NETWORK INSIGHT CLOUD™

Overview: VMware vRealize® Network Insight Cloud™ is a network and security analysis service, purpose-built for SDDCs, branch locations, and public clouds. The service provides comprehensive network visibility and granular understanding of traffic flows between applications to enable cloud security planning and network troubleshooting. Best practices checks, as well as intuitive user interface and search capabilities, simplify monitoring and administration of a customer's network traffic, making it easier for cloud administrators to manage and troubleshoot cloud deployments at scale.

Purchase and Use Restrictions:

If Customer (i) has previously purchased licenses to VMware vRealize® Network Insight™ (Advanced or Enterprise edition) or to VMware NSX® Data Center Enterprise Plus (the "**Existing Licenses**"), which are VMware on-premises software offerings, and (ii) is current on support and maintenance for those licenses, then:

- Customer may purchase a three-year committed term subscription to vRealize Network Insight Cloud to monitor the same assets as are being monitored by the Existing Licenses.
- Customer must not deploy or use an equivalent number of the Existing Licenses during the Subscription Term for vRealize Network Insight Cloud after a 90-day grace period, beginning on the date when the subscription to either of the above add-on offerings is activated.
- Customer must ensure that it is purchasing the correct version of vRealize Network Insight Cloud to enable the monitoring described above.

Purchasing Entitlements:

Entitlements to vRealize Network Insight Cloud are sold on the following basis:

- Per-CPU basis for customers who wish to use the Service Offering to manage an on-premise and VMware Cloud™ on AWS environments.
- Per-VeloCloud Edge by bandwidth tier (MBPS) basis for customers who wish to use vRealize Network Insight Cloud to monitor the VMware SD-WAN™ by VeloCloud® environment.
- Per-vCPU basis for customers who wish to use vRealize Network Insight Cloud to manage their public cloud environments.
- Per Network Device, when purchasing entitlements to vRealize Network Insight Cloud Assurance and Verification, or otherwise when purchasing entitlements to vRealize Network Insight Cloud. "**Network Device**" means a third-party firewall, router, switch, or load balancer which is identified by an IP address.

For purposes of this Section 2.30, "**vCPU**" is defined as a single computational unit of a processor, which may be presented as one or more vCPUs, but may be named differently by public cloud vendors. For example, AWS defines vCPU as "vCPU", but Microsoft Azure defines vCPU as "Core" or "vCPU".

For each vRealize Network Insight Cloud subscription purchased on a per-CPU basis, Customer may use vRealize Network Insight Cloud to monitor one Network Device for each CPU covered by the subscription. If Customer wishes to monitor additional Network Devices, Customer must purchase the appropriate number of subscriptions to VMware vRealize Network Insight Cloud Assurance and Verification.

If Customer purchases an entitlement to VMware vRealize® Network Insight Cloud Assurance and Verification™, it may use that offering for up to the number of Network Devices for which Customer has paid the applicable license fees.

If Customer uses vRealize Network Insight Cloud to monitor its VMware SD-WAN™ environment, Customer may only use vRealize Network Insight Cloud in conjunction with a deployment of VMware SD-WAN and at the same bandwidth tier as that deployment. Customers that want end-to-end network visibility (across data center and branch locations) must purchase entitlements to both (i) vRealize Network Insight Cloud and (ii) vRealize Network Insight Cloud for VMware SD-WAN.

Usage Metering:

For on-premises and VMware Cloud on AWS environments, all CPUs in all hosts managed by the VMware vCenter Server(s) that Customer has added as Data Source(s) in vRealize Network Insight Cloud will be metered as usage of vRealize Network Insight Cloud. Customer cannot specify a subset of a VMware vCenter Server environment (such as clusters(s), folder(s) or host(s)) to be managed by vRealize Network Insight Cloud.

2.31 VMWARE vREALIZE® NETWORK INSIGHT™ UNIVERSAL™

Overview: VMware vRealize® Network Insight™ Universal™ is a cloud-managed subscription offering that includes both on-premises and hosted components. vRealize Network Insight Universal gives customers the ability to holistically manage instances across hybrid and multi-cloud environments, and provides customers with an option to change between their on-premises environment and a cloud environment. vRealize Network Insight Universal (Standard) also provides VMware vRealize® Cloud Federated Analytics™ for a single pane of glass view and control of all a customer's managed environments. The on-premises components of vRealize Network Insight Universal are subject to the General Terms and the Software Exhibit.

Cloud Upgrade Program, Subscription Upgrade Program:

If Customer receives its entitlement to vRealize Network Insight Universal through the VMware Cloud Upgrade Program, Customer agrees that it will, within 90 days of the purchase of the entitlement, relinquish its entitlements to relevant perpetual licenses for the on-premises vRealize Network Insight software product that were exchanged through the vRealize Network Insight Universal Subscription Upgrade Program (the "**Exchanged Licenses**"). By the end of that

90-day period, Customer must stop using any license keys related to the Exchanged Licenses, and VMware will invalidate the license keys for the Exchanged Licenses. Customer is not required to uninstall any on-premises VMware Software if Customer converts its existing perpetual on-premises licenses to a vRealize Network Insight Universal entitlement by applying vRealize Network Insight Universal license key to Customer's existing VMware Software instances.

Expiration of Subscription Term:

Committed term subscriptions for the vRealize Network Insight Universal service do not renew at the end of the purchased subscription term. If Customer does not purchase a new subscription and there is no other active subscription associated with Customer's account, Customer's entitlement to the components and features of the service will be terminated, except that Customer can still access vRealize Network Insight Cloud, which will continue to operate as a separate cloud service offering, and Customer will be charged for use of that service: on an on-demand basis, at the then-current charges for on-demand usage.

2.32 VMWARE vREALIZE® OPERATIONS CLOUD™

Overview: VMware vRealize® Operations Cloud™ is a cloud delivered service that allows a customer's infrastructure and operations teams to manage the enterprise's VMware Cloud™ environment, whether in the customer's own on-premises SDDC or in the customer's hosted environment, such as VMware Cloud™ on AWS. vRealize Operations Cloud provides automated workload optimization, capacity and cost management, and planning and integrated compliance while unifying monitoring across private, hybrid, and public clouds.

The resources deployed and managed in the service are provisioned on private and public cloud platforms configured by VMware. For managing a VMware SDDC, customers will need to download the vRealize Operations Cloud proxy onto their on-premises VMware vCenter® instance.

Use of Pendo:

Hosted components of vRealize Operations Cloud use Pendo functionality to collect data directly from any browsers used to access and use the service. Pendo collects data regarding use of vRealize Operations Cloud, including user interaction and behavior. The data collected and inferred is used by VMware to diagnose and improve its products and services, and to address issues. Users wishing to opt out can do so within the service. Customer agrees to provide the information, above, regarding Usage Data, and Pendo usage, to all Users of vRealize Operations Cloud.

Subscription Upgrade Program:

If Customer receives its entitlement to vRealize Operations Cloud through the VMware Subscription Upgrade Program for vRealize Operations Cloud, Customer agrees to relinquish its entitlements to corresponding VMware vRealize® Operations™ on-premises perpetual licenses. Customer must not use any license keys related to those on-premises perpetual licenses, and VMware will invalidate those perpetual license keys.

2.33 VMWARE vSAN+™

Overview: VMware vSAN+™ provides customers with a consolidated view of their VMware vSAN™ estate, and allows customers to centrally monitor events, alerts, resource capacity, and identify unaddressed security vulnerabilities. Customers can also update VMware vCenter Server® appliances with a single click.

vSAN+ has the following components:

- vSphere version 7.0U3 or above installed in the customer's on-premises environment
- vCenter Server appliance 7.0 U3p05 or above installed in the customer's on-premises environment
- VMware vCenter Cloud Gateway deployed in the customer's on-premises environment; this connects the customer's on-premise vSphere instance and the vCenter Server appliance to the VMware Cloud Console (the "VMC Console")
- Access to vSAN+ services, which are hosted by VMware, through the VMC console

NOTE: As a condition for purchasing a subscription to vSAN+, you must have an existing subscription to vSphere+; that is, you cannot purchase a subscription to vSAN+ as a standalone offering. The number of vSphere+ cores must be the same as or greater than the number of vSAN+ cores.

Subscription Upgrade Program:

If you receive your entitlement to vSAN+ through a VMware subscription upgrade program, then you must, within ninety (90) days of the purchase of the entitlement, relinquish your entitlements to any relevant vSAN perpetual licenses that were exchanged through the subscription upgrade program (the "Exchanged Licenses"). By the end of that 90-day period, you must stop using any license keys related to those specific Exchanged Licenses, and VMware will invalidate the license keys for those Exchanged Licenses.

2.34 VMWARE vSphere+™

Overview: VMware vSphere+™ provides customers with a consolidated view of their VMware vSphere® estate and allows customers to centrally monitor events, alerts, resource capacity, and identify unaddressed security vulnerabilities.

vSphere Advantage has the following components:

- vSphere version 6.5 or above installed in the customer's on-premises environment
- vCenter Server appliance 7.0 U3a or above installed in the customer's on-premises environment
- VMware vCenter Cloud Gateway deployed in the customer's on-premises environment; this connects the customer's on-premise vSphere instance and the vCenter Server appliance to the VMware Cloud Console (the "VMC Console")
- Access to vSphere+ services, which are hosted by VMware, through the VMC console

Subscription Upgrade Program:

If Customer receives its entitlement to vSphere+ through a VMware subscription upgrade program, then Customer must, within 90 days of the purchase of the entitlement, relinquish its entitlements to any relevant vSphere on-premises perpetual licenses that were exchanged through the subscription upgrade program ("Exchanged Licenses"). Customer must stop using any license keys related to the Exchanged Licenses, and VMware will invalidate the license keys for those Exchanged Licenses.

Data Retention and Deletion:

Data retention and deletion policies associated with Customer Content in the service (including any personal data stored within Customer Content) are solely managed by Customer. VMware does not back up the Customer Content and therefore will not be able to recover any of Customer Content in any unforeseen event. Customer is responsible for implementing tools, products, and operational procedures to support data migration, data protection, backup/archive, and restoration for all Customer Content and all configurations created by Customer, including virtual machines and content libraries.

Any deletion of a host on VMware Cloud results in an automated cryptographic wipe of the hard drive, which is performed via destruction of keys used by the self-encrypting drives. This cryptographic erasure ensures that there is no customer content on the drives before returning the servers to the pool of available hardware to be reprovisioned or decommissioned from

service. Service Operations Data and Usage Data is backed up by VMware. A storage policy enforces retention of three years and automatically purges log events that exceed the three-year lifecycle.

If Customer wishes to obtain log data associated with its use of the service, Customer must file a support request and get all the logs required before the effective date of termination of the Subscription Term. Otherwise at the end of the Subscription Term, all data will be deleted.

2.35 VMWARE WORKSPACE ONE®

Overview: VMware Workspace ONE® is a platform made up of a set of cloud services designed to deliver and manage any application on any device. Depending on the edition of Workspace ONE that Customer purchases, the Customer's entitlement may consist of VMware Workspace ONE® UEM for device management, an access policy and identity management service powered by Workspace ONE® Access™ (previously known as VMware Identity Manager), and several sub-service components. Depending on the edition, the service may include access to certain VMware Unified Access Gateway™ components which may need to be installed in Customer's on-premises environment. Customer will also have access to the VMware Enterprise Systems Connector™. Customer may use the service for up to the number of Named Users or Devices for which Customer has paid the applicable fees.

Each edition of Workspace ONE includes entitlements to use different functionality and inclusions. For the selected edition of the service, Customer may only use the functionality entitled for that edition. See the Workspace ONE edition comparison guides, at the URLs listed below, for additional information:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/workspace-one/vmw-workspace-one-edition-comparison-guide.pdf

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/workspace-one/workspace-one-editions-comparison.pdf

When a Device communicates with the Workspace ONE console, it results in transmission of data to and from the Device. That transmission may result in additional charges from Customer's carrier or service provider. VMWARE DISCLAIMS ANY LIABILITY FOR, AND IS NOT RESPONSIBLE FOR, ANY CARRIER OR INTERNET SERVICE PROVIDER DATA COSTS OR CHARGES CUSTOMER MAY INCUR IN CONNECTION WITH ITS USE OF THE SERVICE OFFERING.

Notwithstanding anything to the contrary in the General Terms, the Cloud Exhibit, and any Order, the following terms apply:

- For Workspace ONE Express, Standard, and Advanced editions, the Subscription Term and the applicable billing period will begin within 24 hours after the date on which Customer's instance of the service has been provisioned.
- For Workspace ONE Enterprise, VMware will provision Customer's instance of the service within 14 days after the date VMware books the Order. VMware can elect to delay the start of the billing period at its discretion.

Definitions:

For purposes of this Section 2.34, the following terms have the following meanings:

"Device" means any client hardware, such as a mobile device, that enables installing and running of Workspace ONE on that client hardware.

"Enrolled Device" means any Device that has Workspace ONE installed and that is enrolled in the UEM console, and is being managed by Workspace ONE.

"Named User" means Customer's employee, contractor, or Third-Party Agent who has been identified and authorized by Customer to use Workspace ONE.

"Seat" means an entitlement for (i) one Named User, if the order is on a per-Named User basis, or (ii) one Device, if the Order is on a per-Device basis.

"Third-Party Agent" means a third party delivering information technology services to Customer pursuant to a written contract with Customer.

"User" is defined in the General Terms.

Entitlements

Customer may purchase an entitlement to Workspace ONE on a per-Named User basis or on a per-Device basis. A single order may include both models. Customer is entitled to use Workspace ONE for up to the number of Named Users or Devices for which Customer has paid the applicable fees. Customer can transfer Workspace ONE entitlements from one Named User to another Named User, or from one Device to another Device, within Customer's organization, as long as customer does not exceed the number of Named Users or Devices for which Customer has paid the applicable fees. If Customer enrolls more Devices in the UEM Console than the number of Devices for which Customer has paid the applicable fees, or if Customer has more Named Users than are covered by the fees that Customer has paid, VMware reserves the right to bill Customer for any additional fees incurred, in addition to any other right VMware has under the Agreement.

Per Named User Entitlements:

If Customer has purchased its entitlement to Workspace ONE on a per-Named User basis, the service can be used on the agreed number of Devices for each Named User. Customer may not enroll more Devices than the number of Devices permitted to all Named Users in the aggregate. If Customer exceeds that number, Customer must pay for the extra Enrolled Devices. Each Named User may also access Workspace ONE using web-only access, which will not constitute use of a Device by that user.

If Customer has purchased entitlements to the VMware Workspace Security™ offerings on a per-Named User basis, those entitlements can only be used on an endpoint device that is assigned to a Named User. Per-Named User entitlements cannot be deployed to servers.

Per Device Entitlements:

If Customer has purchased entitlements to Workspace ONE on a per-Device basis:

- Customer cannot use the service to access the Workspace ONE web-based portal from an unmanaged Device (that is, Devices that were never enrolled in, or that have been unenrolled from, the Workspace ONE UEM console).
- Workspace ONE can only be used with Devices being managed by Workspace ONE.

Entitlement Utilization:

Entitlement utilization (to confirm Customer's compliance with its purchased entitlements) is measured as set forth below:

Workspace ONE Component	Per-Device Order Compliance Unit of Measure	Per-Named User Order Compliance Unit of Measure
Workspace ONE UEM	Enrolled Devices	Named Users are entitled to "N" Enrolled Devices*
Workspace ONE Assist	Enrolled Devices	Named Users are entitled to "N" Enrolled Devices*
Workspace ONE Intelligence	Enrolled Devices	Named Users are entitled to "N" Enrolled Devices*

"N" means the number of Enrolled Devices permitted per Named User.

VMware AirWatch®:

If Customer has migrated or converted from a VMware AirWatch® product to Workspace ONE (whether as part of a VMware migration offering, purchase of support and subscription services for Workspace ONE, or receipt of a Workspace ONE entitlement from VMware), use of Workspace ONE (including the applicable Workspace ONE UEM functionality that Customer is using pursuant to the AirWatch terms) is subject to the Agreement, and any legacy terms governing the Workspace ONE UEM functionality will no longer apply.

Security Updates and Maintenance:

Some updates to Workspace ONE may be required for security or stability reasons, including for issues that may affect all Users. In most cases, customers (including customers who have enrolled in the managed hosting service, discussed below) will be given a minimum of five business days' notice for production updates, three business days' notice for trials, and one business day notice for UAT, in advance of the update. However, critical security vulnerabilities updates may be implemented by VMware with no advance notice.

VMware Workspace ONE® Access™:

Customer's subscription to Workspace ONE includes an entitlement to use the VMware Workspace ONE® Access™ service. Customer may use this entitlement to Workspace ONE Access only with Workspace ONE.

VMware Workspace ONE® Verify:

Customer acknowledges that Workspace ONE includes VMware Workspace ONE® Verify, VMware's multi-factor authentication solution included in Workspace ONE Access that is powered by a third-party service provider. If Customer elects to use Workspace ONE Verify, then VMware, its affiliates and its third-party service providers will have access to personal information, including the name, phone number and email address of individual Users. VMware, its affiliates, and its service providers will use the personal information collected through Workspace ONE Verify to provide the multi-factor authentication service.

VMware Workspace ONE® Intelligence™:

VMware Workspace ONE® Intelligence™ is included the Workspace ONE Enterprise and the Workspace ONE Enterprise for VDI editions, and is available as an add-on offering to customers that have purchased entitlements to the Workspace ONE Standard or Workspace ONE Advanced editions, for both Named User and Device entitlements. Workspace ONE Intelligence manages a customer's Devices, and aggregates and analyzes data from the Devices. Workspace ONE Intelligence collects data directly from the mobile apps and/or Devices using Workspace ONE, such as configuration, performance, usage, and consumption data, to provide Workspace ONE. To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with the VMware Privacy Notices, found at https://www.vmware.com/help/privacy.html.

VMware collects data regarding use of the service ("**Customer Data**") and of the customer applications ("**App User Data**"). VMware has the right to use, reproduce, and distribute Customer Data and App User Data when it is aggregated with other information and not specifically identifiable to Customer or to any app user to publish reports (either for the general public or VMware customers) on various metrics of interest, for particular industry sectors, or otherwise. VMware also has the right to use Customer Data and App User Data for data analysis, benchmarking, and machine learning to run models so VMware can derive insights and add intelligence to automation functionality (e.g., anomaly detection, forecasting, or predicting future data, as well as recommending possible corrective actions).

In connection with Customer's use of Workspace ONE Intelligence, Customer may elect to integrate and use an offering from a partner in the VMware Workspace ONE® Trust Network (each a "**TN Partner**"). If Customer elects to use a solution provided by a TN Partner (a "**TN Solution**") in combination with Workspace ONE Intelligence, data collected by the TN Solution ("**TN Solution Data**") will be sent to Workspace ONE Intelligence to provide the Workspace ONE Intelligence offering. VMware may use any TN Solution Data to improve its products and services, and other purposes as set forth in the Agreement. The TN Solution is considered Third-Party Content under the Agreement, and any data transferred between the TN Partner and VMware will be governed by each party's respective agreement with Customer.

Hub Services:

Hub Services is a set of services provided by Workspace ONE Access that adds functionality to Workspace ONE. Hub Services provides Users with a single destination to access Customer's corporate resources. Hub Services includes the Workspace ONE applications catalog, notifications, and people search features. Any customer that has purchased an entitlement to Workspace ONE, either as an on-premises software offering or as a cloud service, can use Hub Services. Customers that have purchased an entitlement to the Workspace ONE cloud service can utilize Hub Services through their existing Workspace ONE Access tenant. Hub Services is included in all editions of the Workspace ONE cloud service.

VMware Workspace ONE® Assist™:

VMware Workspace ONE® Assist™ is an add-on offering to Workspace ONE, that enables IT and help desk staff to remotely access and troubleshoot a covered Device, in real time, to support productivity. Workspace ONE Assist provides the ability to accept, pause, and end a remote session at any time, for enhanced privacy. A separate agent is required to be installed on a covered Device, through Workspace ONE UEM on the Android, Windows 10, MacOS, and Windows CE operating systems. The capabilities are embedded in the Workspace ONE Intelligent Hub application on iOS.

VMware Workspace ONE® mobile flows:

The VMware Workspace ONE® mobile flows feature is included in Workspace ONE Enterprise and Enterprise for VDI editions (the hosted offerings, not in the Workspace ONE on-premises offering), as well as in the Workspace ONE Intelligence add-on service. Workspace ONE mobile flows helps employees perform tasks across multiple business back-end systems from a single app (like VMware Workspace ONE® Intelligent Hub), eliminating the need for end users to visit multiple websites or apps while performing business tasks. For example, an employee who receives approval requests from Concur in Workspace ONE Intelligent Hub, can approve/deny them directly from Workspace ONE Intelligent Hub without having to go to the Concur application.

NOTE: VMware plans to discontinue support for Mobile Flows at the end of August 2022.

VMware Workspace Security™:

The VMware Workspace Security™ offerings include VMware Carbon Black Cloud™ platform functionality in combination with Workspace ONE and VMware Horizon Service capabilities.

VMware Horizon Cloud Service for Application Virtualization:

Workspace ONE Enterprise includes an entitlement for the Horizon Cloud Service for application virtualization.

Managed Hosting Service:

The Workspace ONE managed hosting service is designed to provide the functionality of the Workspace ONE cloud service but allows a customer to control its own upgrade cadence for major version upgrades of Workspace ONE UEM.

The Workspace ONE managed hosting service can be purchased by eligible customers. For the managed hosting service, the customer can specify the data center region where its environment will be hosted, based on the then-current list of available data center locations. If the customer moves its Workspace ONE instance from one data center to another, the customer may be required to re-enroll its Devices. With the managed hosting service (but not with the shared environment hosting service), the customer can schedule timing of software updates to the environment based on a list of available time slots. Managed hosting customers may delay or forego upgrades (subject to the remaining portions of this section), but support is limited to supported versions of the Workspace ONE UEM service, as specified in the then-current VMware product lifecycle matrix, found at: https://lifecycle.vmware.com/

VMware requires customers to be on supported versions of Workspace ONE UEM to maintain the functional integrity and security posture of the hosted platform; supported versions of Workspace ONE UEM are eligible to get critical security and application updates on an on-going basis.

Managed hosting customers will receive notifications 60 days and 30 days prior to a version of Workspace ONE going out of support and will be requested to schedule an upgrade to a supported version. Customers who have not scheduled updates to remain compliant with the VMware product lifecycle matrix will be required to upgrade before receiving further support from VMware. VMware reserves the right to schedule an upgrade for a managed hosting customer that is on an unsupported version, and the right to proceed with the upgrade of the customer's environment to a supported version, if the customer does not comply with the requirement to schedule the upgrade.

Managed hosting customers are also subject to VMware's processes regarding critical security upgrades, which may be implemented with minimal or no advance notice.

Perpetual + Hosting:

Customers (i) that purchased perpetual licenses of the on-premises Workspace ONE Standard and Workspace ONE Advanced software offerings (the "Software") prior to January 2018 and (ii) that also purchased an entitlement to hosting those perpetual licenses prior to January 2018, would have been eligible to elect either a shared hosting environment or a managed hosting service, as described above, allowing the customer to use the Software in a production environment via Internet-based consoles. These services are included here, for clarity, and are not available to customers who do not meet eligibility parameters (i.e., purchasing both perpetual license and a hosting entitlement prior to January 2018). A customer enrolled in shared environment hosting or managed service hosting cannot migrate from one environment to the other during a Subscription Term. If a customer wants to change its hosting service entitlement, it must contact VMware to determine available migration options. VMware does not guarantee that migration will be possible.

Eligible Workspace ONE perpetual license customers (as described above) may choose to operate one or more components of Workspace ONE in their on-premises environment, with the remaining Workspace ONE functionality operating in the Workspace ONE hosted environment. However, customers may not mix on-premises installation and VMware hosting services for the same component of Workspace ONE; for example, all instances of the Workspace ONE UEM console must be all on-premises or all in the VMware hosted environment. The customer must not use the Software, through the Workspace ONE service, in a way that exceeds the customer's license entitlements (e.g., user/device limitations, applicable third-party terms, etc.) as set forth the applicable Order, and as set forth in the Agreement. If there is a conflict between the (i) Cloud Services Exhibit and this Services Guide, on the one hand and (ii) the Software Exhibit and the Product Guide, on the other hand, then the Cloud Services Exhibit and this Services Guide will control with respect to the service: https://www.vmware.com/download/eula/product-guides.html

Standard VMware support and subscription services ("SnS") must be purchased for each Workspace ONE perpetual license that is hosted. SnS must be kept current at all times during the hosting service subscription term. The provisions of the General Terms, the Software Exhibit, and the Product Guide continue to apply to the perpetual licenses (e.g., user/device limitations, etc.).

Hosting Services – Latest Mode:

Customers that purchased a "latest mode" license as part of a VMware Subscription Upgrade Program will forego the ability to control updates and will be upgraded to the latest version as per VMware's standard hosted offering.

VMware Advanced Monitoring powered by ControlUp – Optional Add-on:

VMware Advanced Monitoring powered by ControlUp is a third-party solution that delivers a real-time monitoring and visualization engine for VMware Horizon that allows customers to have a unified console for monitoring, triggers and alerts, troubleshooting, and automation for their Horizon deployment. VMware Advanced Monitoring allows customers to monitor their entire VMware Horizon environment, detect anomalies, and proactively solve issues across their deployment. VMware Advanced Monitoring has an analytics engine that provides insights and reporting on the data that is collected from the customer's environment. VMware Advanced Monitoring is hosted by ControlUp, Inc., from its data centers. VMware Advanced Monitoring can be purchased as an add-on for Workspace ONE Enterprise and Workspace ONE Enterprise for VDI.

If Customer purchases an entitlement to VMware Advanced Monitoring, Customer must purchase an equivalent number of Seats for VMware Advanced Monitoring as it has purchased for the applicable Workspace ONE service.

VMware will provide support for VMware Advanced Monitoring. The Agreement will govern Customer's use of the VMware Advanced Monitoring, and will supersede any terms presented to Customer during the deployment and sign-in process for VMware Advanced Monitoring. Notwithstanding anything in the Agreement, and other than as expressly set forth in this section, VMware provides the VMware Advanced Monitoring offering without any indemnification or warranty whatsoever.

Experience Workflows™ for VMware Workspace ONE® powered by Boomi - Optional add-on:

Experience Workflows™ for VMware Workspace ONE® powered by Boomi is an optional add-on feature available for Hub Services. Experience Workflows helps employees perform tasks across multiple business back-end systems from VMware Workspace ONE® Intelligent Hub, eliminating the need for end users to visit multiple websites or apps while performing business tasks. For example, an employee who receives approval requests from Concur in Workspace ONE Intelligent Hub, can approve/deny them directly from Workspace ONE Intelligent Hub without having to go to the Concur application.

Mobile Threat Defense - Optional add-on:

VMware Workspace ONE® Mobile Threat Defense™ is an optional feature that helps organizations ensure their mobile devices are secure by analyzing device, operating system, application, web, and network data to identify security threats and vulnerabilities. Threats are visible to IT and security administrators through the Workspace ONE Mobile Threat Defense administrative console, where administrators can also define policies to automatically take remediation actions against vulnerable Devices. Workspace ONE Mobile Threat Defense integrates with Workspace ONE UEM to synchronize Devices across services, and perform remediation actions, and with Workspace ONE Intelligence to synchronize threat events that can be used to generate dashboards and reports for a single pane of glass into the management and security of mobile endpoints.

Workspace ONE Mobile Threat Defense is hosted by Lookout, Inc. in the AWS US-West Region. Threat data captured from Devices that have activated the Workspace ONE Mobile Threat Defense service may be used by Lookout, Inc for security research and to improve its ability to detect new threats. You consent to such processing by Lookout, Inc. for its purposes. Refer to the Lookout Privacy Notice at: https://legaldocs.lookout.com/en/enterprise-privacy-policy.pdf, the Workspace ONE Privacy Disclosure at https://www.vmware.com/help/privacy/uem-privacy-disclosure.html, and end user disclosures within the mobile app.

VMware will provide support for the Workspace ONE Mobile Threat Defense offering. VMware terms govern Customer's use of Workspace ONE Mobile Threat Defense and will supersede any terms presented to Customer during the deployment and sign-in process for Workspace ONE Mobile Threat Defense.

VMware SaaS App Management™ by BetterCloud – Optional add-on:

VMware SaaS App Management™ by BetterCloud add-on is an optional feature available in the United States only. VMware SaaS App Management delivers a SaaS Management Platform (SMP) that helps organizations discover, manage, and secure SaaS apps across their environments with a single platform, eliminating the need for IT admins to use multiple consoles. The service is hosted by BetterCloud, in its United States-based data center.

VMware SaaS App Management includes three modules which are sold as separate offerings: Discover, Manage, and Secure. Customer has access up to 10 apps integrations, which can be out-of-the-box integrations available in the BetterCloud Integration Center, or custom integrations through the BetterCloud API. The offering also includes an implementation service package delivered by the BetterCloud professional services team to help customers succefully onboard.

Entitlements to the offering are sold on a per end user account/per month and must be licensed for the customer's entire user base. The number of entitlements to the SaaS App Management offering must equal the number of Workspace ONE entitlements (whether per Named User or per Device). Support for VMware SaaS App Management can be obtained from VMware, or directly from BetterCloud through in-product live chat with BetterCloud, or through web form or email to support@bettercloud.com.

Data Retention and Deletion:

Termination of a Customer's entitlement due to expiration, termination, cancellation, or any other cause will result in loss of access to the Workspace ONE UEM Console, discontinuation of software updates, account services, support, and deletion of such environments, configurations, and data. Data from a terminated entitlement will be deleted within 90 days of a deletion request.

Subscription Upgrade Program:

If Customer receives its entitlement to Workspace ONE under the VMware Subscription Upgrade Program for Workspace ONE, Customer agrees to (i) relinquish its entitlements to any corresponding perpetual licenses for the on-premises Workspace ONE software product and (ii) complete migration to the Workspace ONE service, within 90 days after the effective date of the relevant agreement (e.g., an Enterprise License Agreement ("**ELA**"), or an amendment to an ELA, etc.). Failure to complete the migration within 90 days will result VMware ceasing support for Customer's on-premises Workspace ONE instance, and Customer will have no further access to upgrade and installer files for Customer's on-premises instance of Workspace ONE. After Customer has completed the migration to the Workspace ONE service, Customer must not use any license keys related to the perpetual licenses for the on-premises Workspace ONE software product, and VMware will invalidate those license keys.

2.36 VMWARE WORKSPACE ONE® ACCESS™

Overview: VMware Workspace One® Access™ (formerly known as VMware Identity Manager™) provides an integrated platform for users to access their applications and data on any of their devices. With Workspace One Access, a customer's IT department can manage entitlements and policy controls from a single management console. If Workspace ONE Access is used with Workspace One Unified Endpoint Management in an on-premises environment, Customer's use is governed by the General Terms, the Software Exhibit, and the Product Guide.

Hub Services:

Hub Services is a set of services that are co-located with Workspace ONE Access that add functionality to Workspace ONE. Hub Services provide Users with a single destination to access Customer's corporate resources. Hub Services includes the Workspace ONE applications catalog, notifications, and people search features. Any customer that has purchased an entitlement to Workspace ONE, either as an on-premises software product or as a cloud service can use Hub Services. Customers who have purchased an entitlement to the Workspace ONE cloud service can utilize Hub Services through their existing Workspace ONE Access tenant. Hub Services is included in all editions of the Workspace ONE cloud service.

Data Retention and Deletion:

Full termination of a Customer's entitlement due to expiration, termination, cancellation, or any other cause will result in loss of access to the UEM Console, discontinuation of software updates, account services, support and a deletion of such environments, configurations, and data pursuant to applicable VMware policies. Data from a terminated entitlement will be deleted within 90 days of a deletion request.

2.37 VMWARE WORKSPACE ONE® INTELLIGENCE™ FOR CONSUMER APPS

Overview: VMware Workspace ONE® Intelligence™ for Consumer Apps enables customers to monitor and optimize application performance and improve user engagement through actionable app insights. The service provides customers with a mobile app SDK (Software Development Kit) that helps gather app performance data, and access to a cloud-based VMware Workspace ONE® Intelligence™ console to view insights based on the collected data.

Data Collection:

VMware collects data regarding Customer's use of the service ("**Customer Data**") and App Users' use of the Customer App(s) ("**App User Data**"). VMware has the right to use, reproduce, and distribute Customer Data and App User Data when it is aggregated with other information and not specifically identifiable to Customer or to any App User, to publish reports (either for the general public or VMware customers) on various metrics of interest, for particular industry sectors or otherwise. VMware also has the right to use the Customer Data and App User Data for data analysis, benchmarking, and machine learning to run models so VMware can derive

insights and add intelligence to automation functionality (e.g., anomaly detection, forecasting, or predicting future data, as well as recommending possible corrective actions). As used in this Section 2.36, "**App User**" means a user of the Customer App(s). "**Customer App(s)**" means the customer's mobile applications identified in the relevant Order.

3. CHANGE LOG

Date	Section	Offering	Change
28 June 2022	1	Terms Applicable to All VMware Cloud Services	Added paragraph on authorizations, compliance.
28 June 2022	2.34	VMware Workspace ONE	Added clarification re data deletion.
28 June 2022	2.35	VMware Workspace ONE Access	Added clarification re data deletion.
12 July 2022	2.26	VMware vCloud Usage Insight	Service deprecated; entry content deleted.
12 July 2022	2.34	VMware Workspace ONE	Added clarification on entitlements and enforcement, added descriptions of optional add-on services.
12 July 2022	2.33	VMware vSphere+	Updated name of service from VMware vSphere Advantage to VMware vSphere+
25 July 2022	2.37	VMware vSAN+	Added section for this offering.
17 August 2022	2.8	VMware Cloud Disaster Recovery	Added section on PCI compliance for the service