Specific Program Documentation ("SPD") and SaaS Listing

VMware Live Recovery

The Broadcom software program(s) ("Software") and SaaS offering(s) ("SaaS Offering") listed below are provided under the following terms and conditions in addition to any terms and conditions referenced on the Broadcom quote, order form, statement of work, or other mutually agreed ordering document (each a "Transaction Document") under the applicable end user agreement or governing contract (collectively, the "Agreement") entered into by the Customer and the Broadcom entity ("Broadcom") through which the Customer obtained a license for the Software and SaaS Offering. These terms shall be effective from the effective date of such Transaction Document. Capitalized terms have the meanings ascribed to them herein, or, otherwise, in the Agreement.

The version of the SPD published on legaldocs.broadcom.com on the date that Broadcom accepts the Customer's Transaction Document for Software applies to the version of Software in that Transaction Document. If the Customer installs a release of Software that Broadcom provides as part of Support services, then the then-current version of the SPD published on legaldocs.broadcom.com on the date the Customer installs that release applies to that release of Software.

The then current version of the SaaS Listing and published on legaldocs.broadcom.com applies to the SaaS Offering. Broadcom may from time to time make modifications to the SaaS Offering and/or any part of the SaaS Listing. Any changes will become effective on the date published or as Broadcom may notify the Customer. Broadcom may also elect to cease providing the SaaS Offering, in which case Broadcom will provide notice pursuant to applicable Broadcom policies. If Broadcom deprecates any material feature or functionality of the SaaS Offering or makes a change that has a material, detrimental impact on the Customer use of the SaaS Offering, Broadcom will notify the Customer prior to the effective date of that change. If the Customer elects to terminate their entitlement to the SaaS Offering because of the material, detrimental change, Customer must notify Broadcom no later than 30 days after our notice date. Customer's notice must state the effective termination date, which must not be more than 90 days after the date of their notice, unless the Customer and Broadcom agree to a longer period. Customer will be responsible for all fees incurred prior to the effective termination date or end of availability. Broadcom will refund any prepaid fees prorated as of the effective termination date, as the Customer's sole and exclusive remedy for any termination/cessation of the SaaS Offering.

This document serves as the SPD for VMware Live Site Recovery protection technology and VMware Cloud Director Availability protection technology and as the SaaS Listing for VMware Live Cyber Recovery protection technology. The terms of this document applicable to VMware Live Site Recovery protection technology and VMware Cloud Director Availability protection technology are referred to as the SPD. The terms of this document applicable to VMware Live Cyber Recovery protection technology are referred to as the SaaS Listing.

Program Name: ***VMware Live Recovery***

1. DEFINITIONS.

All terms defined in the VMware Licensing Glossary published on https://docs.broadcom.com/doc/vmware-licensing-glossary apply to this SPD and SaaS Listing unless specified herein.

"**Tebibyte**" means a unit of physical storage capacity that is equal to 2^40 bytes.

"**Protected Capacity**" means the sum of the logical (used) storage size of all protected virtual machines and all incremental cloud backups (snapshots) on VMware Live Cyber Recovery protection technology.

"**Protected Virtual Machine**" means the number of Virtual Machines being replicated using VMware Live Recovery, regardless of whether the VMs are currently powered on.

"Recovery Time Objective" means the period of time beginning when the Customer initiates a failover of a vSphere workload protected by VMware Live Cyber Recovery protection technology to the time when that workload starts powering on in a recovery SDDC.

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

2. USE RIGHTS AND LIMITATIONS.

- VMware Live Recovery grants Customer the rights to deploy any of of the following protection technologies:
  - VMware Live Site Recovery: On-premises disaster recovery Software;
  - VMware Cloud Director Availability: On-premises disaster recovery Software; and
  - VMware Live Cyber Recovery: Cloud-based disaster recovery service.

- VMware Live Recovery is licensed based on the number of protected Virtual Machines (VMs). Customer must purchase a license for each protected VM by any of the VMware Live Recovery protection technologies. If a VM is protected by multiple technologies (e.g., VMware Live Site Recovery and VMware Live Cyber Recovery), Customer must purchase two quantities of VM licenses. Additional licensing details for each protection technology are provided below.

- VMware Live Recovery subscription license includes Support Services that may only be used for VMware Live Recovery licensed hereunder.

- VMware Live Recovery may only be used as an add-on to VMware Cloud Foundation (including any partner integrated offering), VMware Cloud Foundation Edge, or VMware vSphere Foundation.

- Customer may use VMware Live Recovery up to the quantity they have purchased. If Customer exceeds this amount, Customer is treated as non-compliant and must immediately purchase additional licenses to cover the excess usage. Broadcom reserves the right to suspend or terminate VMware Live Recovery service if additional quantities to cover usage are not purchased.

- Customer must use VMware Live Recovery, regardless of protection technology, only on Broadcom-supported topologies.

- Customer must have recovery SDDC hosts that are required for VMware Live Recovery to function as designed. These hosts are not included with any VMware Live Recovery purchase.

VMware Live Site Recovery Protection Technology

- VMware Live Site Recovery protection technology must be deployed at both the source and target sites. For uni-directional protection, VMware Live Recovery licensing is needed only for the VMs at the source. For bi-directional protection, VMware Live Recovery licensing is needed for the VMs at both the source and target locations.
- In VMware Live Site Recovery protection technology, after a failover, VMware Live Recovery license will be required if the target VMs have to be protected. VMware Live Recovery licenses used at the source can be used at the target as long as the licenses are no longer being used at the source.

VMware Cloud Director Availability Protection Technology

- VMware Cloud Director Availability protection technology must be deployed at both the source and target sites. For uni-directional protection, VMware Live Recovery licensing is needed only for the VMs at the source or at the target. For bi-directional protection, VMware Live Recovery licensing is needed for the VMs at both the source and target locations.
- In VMware Cloud Director Availability protection technology, after a failover, VMware Live Recovery license will be required if the target VMs have to be protected. VMware Cloud Director Availability licenses used at the source can be used at the target as long as the licenses are no longer being used at the source.

VMware Live Cyber Recovery Protection Technology

- To use VMware Live Cyber Recovery protection technology, protected capacity licenses measured in tebibyte ("TiB") are required, with a minimum purchase of 10 TiB per subscription region. These capacity licenses are in addition to the protected VMs purchased.

- Broadcom reserves the right to bill the Customer for excessive egress data transfers incurred during typical use of the service for replication to the cloud and failback to the original protected site. Excessive is defined as over 50% of the protected VM storage footprint.

- Customer data is stored up to 60 days after the subscription term end date and will be permanently deleted thereafter.

- To facilitate quick recovery of protected virtual machines to a recovery SDDC, VMware Live Cyber Recovery protection technology automatically creates one or more Network File System (NFS) datastores and attaches them to the SDDC. These datastores facilitate the immediate recovery of protected virtual machines, with virtual disk backups continuing to reside on the Scale-out Cloud File System (SCFS). Virtual machines in the SDDC can immediately power on by directly accessing these

datastores either while virtual disk backup data is copied to the VMware vSAN™ datastore on the SDDC (referred to as "Live Mount"), or for an extended period during production failover (referred to as "Running on the Cloud Filesystem"). Virtual Machines running on the SCFS are permitted to use the NFS share in this manner for a maximum of 30 days, after which time all failed-over virtual machine storage must be copied 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 must never be used as general purpose storage. Customer is not permitted to use the vSphere Client, vSphere APIs, or any method other than the interfaces provided by VMware Live 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, Broadcom will not guarantee support for the affected instances of the service.

- The use of Carbon Black or Carbon Black Cloud feature, products and/or technology in conjunction with VMware Live Cyber Recovery protection technology is limited to use within the Isolated Recovery Environment and Ransomware Recovery workflow. Any use of Carbon Black products or technologies in a production setting is strictly prohibited unless those Carbon Black products are properly licensed.

- To deploy VMware Live Cyber Recovery, Customer is required to have VMC on AWS hosts to serve as recovery SDDC hosts. These hosts are not included with any VMware Live Cyber Recovery purchase. For details, refer to VMC on AWS SaaS Listing on legaldocs.broadcom.com.

- **Data Export:**
    - The following data can be exported from the SaaS Offering: VM backups, Guest files, Configurations, Logs (including audit logs)
    - The following data cannot be exported from the SaaS offering: SaaS Infrastructure OS logs

3. SERVICE LEVEL AGREEMENT.

This Service Level Agreement ("SLA") is only applicable to VMware Live Cyber Recovery protection technology.

Availability

Broadcom will use commercially reasonable efforts to ensure that VMware Live Cyber Recovery protection technology is available during a given billing month equal to the "Availability Commitment" specified in the table below.

Service	Availability Commitment
VMware Live Cyber Recovery protection technology	99.9%

If the Availability of VMware Live Cyber Recovery protection technology is less than the Availability Commitment, then Customer may request an SLA Credit. Availability in a given billing month is calculated according to the following formula:

"Availability" = ([total minutes in a billing month – total minutes Unavailable] / total minutes in a billing month) x 100

Disaster Recovery Failover

Broadcom will use commercially reasonable efforts to ensure that a Disaster Recovery Failover ("DR Failover") will meet the specified Recovery Time Objective ("RTO") specified in the table below.

Service	Recovery Time Objective
DR Failover	< 2 hours

The following will be excluded from any calculations related to the RTO:

- Time associated with the Customer's manual action or execution of custom script;
- Time associated with any customization defined by the Customer, such as IP customization;
- Time required to boot up virtual machines; and

- Any wait time for availability of recovery SDDC capacity.

SLA Events

VMware Live Cyber Recovery protection technology will be considered "Unavailable", subject to the SLA Limitations set forth below, if Broadcom's monitoring tools determine one of the following events (each, an "SLA Event") has occurred.

The total minutes that VMware Live Cyber Recovery protection technology is Unavailable for a particular SLA Event is measured from the time that Broadcom validates the SLA Event has occurred, as defined below, until the time that Broadcom resolves the SLA Event such that VMware Live Cyber Recovery protection technology is Available to the Customer.

If two or more SLA Events occur simultaneously, the SLA Event with the longest duration will be used to determine the total minutes Unavailable.

Each of the following will be considered an SLA Event for VMware Live Cyber Recovery protection technology:

- Customer's VMware Live Cyber Recovery protection technology orchestrator user interface is inaccessible for ten consecutive minutes;
- Customer's retained cloud backups in VMware Live Cyber Recovery protection technology are inaccessible for ten consecutive minutes;
- Customer is unable to create or modify protection groups and disaster recovery (DR) plans in VMware Live Cyber Recovery protection technology for ten consecutive minutes;
- Customer is unable to initiate a DR plan as a test or failover in VMware Live Cyber Recovery protection technology for ten consecutive minutes;
- Customer is unable to initiate deployment of a recovery SDDC using VMware Live Cyber Recovery protection technology for ten consecutive minutes, even though recovery SDDC capacity is available in the region; and
- None of the Customer's recovered virtual machines running directly off the Scale-Out Cloud File System ("SCFS") can access the virtual disk storage on the SCFS for ten consecutive minutes.

Availability of VMware Live Cyber Recovery protection technology is dependent on and subject to availability of the underlying services on which VMware Live Cyber Recovery protection technology is hosted. Availability of the underlying services is not covered by the service availability metrics set forth in this SLA. If the underlying services are unavailable, and therefore VMware Live Cyber Recovery protection technology is Unavailable, their sole recourse pursuant to the Agreement is to Broadcom.

SLA Limitations

The following will be excluded from any time-based calculations related to VMware Live Cyber Recovery protection technology being Unavailable:

- Scheduled maintenance where the Customer has been notified at least 24 hours in advance;
- Recurring or zero-impact maintenance that is generally applicable to Customer;
- Customer's misuse of VMware Live Cyber Recovery protection technology or a service component;
- Force majeure events, denial of service attacks, viruses, or hacking attacks for which there is no commercially reasonable known solution, or any other events that are not within our control or that could not have been avoided with commercially reasonable care;
- Acts or orders of government;
- Packet loss, network or internet problems beyond Broadcom's border router supporting our public internet connectivity; and
- Bugs in code or services for which there is no commercially reasonable known fix (even if there is a known workaround).

Broadcom's monitoring tools, data, and records will be the sole source of information used to track and validate Availability. Upon request, Broadcom will provide to the Customer, within 45 days after a confirmed SLA Event, a copy of the Availability report that Broadcom makes generally available to Customer.

SLA Credits

Each "SLA Credit" is an amount equal to the specified percentage of the per-TiB and the per-VM charges (net of any discounts) charged for the billing month in which the SLA event occurred, as specified in the table below:

Monthly Uptime Percentage	SLA Credit Percentage
Less than 99.9% but equal to or greater than 99.0%	10%
Less than 99.0%	30%
Recovery Time Objective for DR Failover	SLA Credit Percentage
< 2 hours	100%

Customer is not eligible to receive any SLA Credits for an SLA Event if any of the following conditions apply:

- Customer did not ensure that their environment meets all prerequisites for the deployment and use of VMware Live Cyber Recovery protection technology, as outlined in the technical documentation. This includes, but is not limited to, ensuring outbound network connectivity from the protected site and configuring an unexpired, properly scoped API token within the VMware Live Cyber Recovery protection technology user interface;
- Customer modified the settings of the SDDC used for recovery of their virtual machines in a manner that disrupts the functionality of VMware Live Cyber Recovery protection technology (e.g., changes to firewall configurations that interrupt access between the SDDC and SCFS or Orchestrator components, or attempts to unmount the Network File System ("NFS") datastores provisioned by VMware Live Cyber Recovery protection technology);
- Customer used the vSphere Client, vSphere APIs, or any method other than the interfaces provided by VMware Live Cyber Recovery protection technology to create and power on virtual machines directly on the NFS datastore created by VMware Live Cyber Recovery protection technology on the recovery SDDC;
- If Customer does not have sufficient recovery SDDC capacity and recovery cluster(s) to support the failover;
- If the SLA was caused by the recovery SDDC offering;
- Customer is delinquent on any payments for VMware Live Cyber Recovery protection technology; and
- The SLA Event occurred due to Customer's failure to meet their security responsibilities, as set forth in this SLA.

To request an SLA Credit, Customer must file a support request within thirty (30) days after the suspected SLA Event or the alleged RTO failure. Broadcom will review the request and issue an SLA Credit when Broadcom validates the SLA Event or RTO failure based on Broadcom's data and records.

SLA Credits will be issued to the person or entity that Broadcom invoices for VMware Live Cyber Recovery protection technology, as a separate credit memo that can be applied towards a future invoice for VMware Live Cyber Recovery protection technology. If the Customer's subscription term for VMware Live Cyber Recovery protection technology expires or is terminated prior to the issuance of a Service Credit, the Service Credit will become void as of the date of the expiration or termination.

The Service Credits specified in this SLA are the Customer's sole and exclusive remedies for any SLA Events or any failure to meet the RTO occurring during their subscription term for VMware Live Cyber Recovery protection technology or for any other claim in connection with this SLA.

4. THIRD PARTY INFORMATION AND TERMS.

- Any required third-party software license terms are incorporated by this reference and are set forth in online documentation at techdocs.broadcom.com or legaldocs.broadcom.com.

- VMware Tools is a suite of utilities and drivers that can be installed in a Guest Operating System to enhance the performance and functionality of a Guest Operating System when running in a Virtual Machine in conjunction with a vSphere hypervisor. Customer may not use VMware Tools with any other hypervisor. Customer may distribute the VMware Tools to third parties solely when installed in a Guest Operating System within a Virtual Machine. Customer is liable for compliance by those third parties with the terms and conditions of the Framework Agreement.