11:11 DRaaS — Azure Service Terms

April 1, 2023

1. DEFINITIONS

"**ATOD**" is at time of disaster.

"**ATOT**" is at time of test.

"**Azure**" is an acronym for Microsoft Azure and their products as described at https://azure.microsoft.com

"**Documentation**" refers to all documentation provided by Provider for the purpose of providing the Services, including, without limitation, the operating manuals, user instructions, technical literature and other related materials supplied to Customer by Provider or its licensor for aiding with the use and application of the Services.

"**Failback**" refers to the necessary activity and components used to move Customer's data back to the production environment after the recovery period.

"**Failover**" refers to the necessary activity and components used to stand up Customer's recovery environment to resume operation.

"**Intellectual Property Rights**" refers to any (and all) registered and unregistered intellectual property rights (e.g., copyright, patents, trademarks, design rights, database and compilation rights, trade secrets, topographies, logos, brands, domain names and goodwill), howsoever arising and in whatever media, including any applications for their protection or registration and all renewals and extensions.

"**Managed Service**" is Provider's access and ability to perform troubleshooting, request fulfillment and changes to Customer's environment on behalf and at the request of Customer.

"**Occupied Data**" describes the storage volume consumed for replicated data on target side, including additional storage for retention.

"**Protected Instance**" is a virtual machine or server per OS being protected for ATOT or ATOD.

"**RPO**" is the recovery point objective, which is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.

“**RTO**” is the recovery time objective, which is the maximum acceptable amount of time since the last data recovery point.

“**Service**” is the service described in an Order, which may be performed by Provider or its designated subcontractors.

“**Snapshot**” is a point in time copy of Customer data that Customer can use as a recovery point.

“**Software**” refers to the third-party software provided by Provider and installed in the Customer system in connection with the provision of the Services.

“**Tear Down**” refers to the process of removing/decommissioning the cloud infrastructure.

“**Usage**” refers to the reported amount of resources, services or management hours used or consumed within the DRaaS — Azure service.

“Tenant / Subscription” refers to a logically isolated, single-tenant virtual construct consisting of VMs, vLANs, virtual load balancers and virtual firewalls committed to Customer within which Customer’s workloads are executed.

“**VM**” refers to a Provider managed virtual machine.

2. FEATURES

Provider’s DRaaS – Azure is a managed recovery solution to replicate and recover x86 virtual systems into and leveraging the power and scale of the Azure cloud platform. The DRaaS – Azure Service includes (where selected on the applicable Order):

a) Fully managed, virtual-to-virtual, hypervisor-based replication and recovery solution for an on-premises virtual server running within VMware/Hyper-V hypervisors.

b) Administration by Provider of the replication onto Azure the infrastructure (as defined below).

c) Support of the initial installation and configuration of replication software and creation of replication subscription and associated compute and storage, and the recovery blueprint on Azure.

d) Administration by Provider of failover activities ATOT or ATOD.

e) Recovery skills and account management within Azure.

f) An RTO of two (2) hours for recovery of 100 VM’s and an additional one (1) for each additional increment of 100 servers. Provider will recover all servers within the Recovery Plan (as defined below), including the availability of the OS ready for Customer to access.

Provider will provide the following, in accordance with the completed customer design requirements (CDR) form, for occupied data and number of Protected Instances identified in the Order:

a) Configuration of the initial recovery plan that is set up for Customer's Occupied Data and Protected Instance(s), including fine tuning the plan that is set up during the initial sixty (60) days following the Start Date of the Order (the "Recovery Plan").

b) Monitoring and management of the automated replication system for Customer's Occupied Data and Protected Instance(s) that reside on Customer-selected Azure services and resources (in the applicable Azure region(s) selected) as detailed in the Order ("Target System").

c) Notification to Customer in the event of a failure to replicate Occupied Data and Protected Instance(s) to the Target System.

d) Hosting of a copy of the Protected Instance(s) and Occupied Data on Azure blob storage services, to be provisioned ATOT or ATOD on Azure instance (hereinafter collectively referred to as "Azure Infrastructure").

e) Perform Failover activity upon Customer's request, allowing Customer to validate use of its data and Event applications following such recovery (each a "Recovery Test"). The number and/or duration of Recovery Tests is identified in the Order.

f) Tear down and deletion of any Azure infrastructure that was provisioned on Customer's behalf at ATOT or ATOD, following the conclusion of a Recovery Test or Event.

g) Subject to the prior agreement of a Failover plan with Provider covering Customer's Failback scenarios, perform Failback activity to Customer's production environment upon Customer's request, following an Activation. Any Provider activities ATOT/D beyond configuration of Failback replication software may incur additional expenses, which will be charged on a time and materials basis.

Provider manages the data replication and Failover. Customer is responsible for any additional recovery steps after the Provider Failover activity (e.g., Provider will not have any log in credentials or access to Customer's Failover environment to perform additional steps, which are out-of-scope for this Service).

Customer will provide its Activation notice to Provider in the manner described in the users' guide. An "Activation" is the notification provided by one of Customer's designated representatives to Provider, indicating that an Event has occurred. An "Event" is any planned or unplanned event or condition that renders Customer unable to use the protected environment for their intended computer processing and related purposes. Provider will provide access to the users' guide via the Customer Portal at https://myportal.sungardas.com/.

Activations are limited to two (2) Activations per month. Additional Activations are invoiced at the then-prevailing rates for time and materials.

3. GENERAL

For Provider to provide the Services to Customer, Customer shall:

a) Provide an accurately completed copy of the CDR form.

b) Procure all the infrastructure including Internet, IP bandwidth or other network bandwidth, environmental controls, and other infrastructure relating to Customer's systems/environment that are needed to support the delivery of Services identified in the Order.

c) Procure and install promptly any necessary third-party software as specified by Provider in the initial Recovery Plan or during the term of the Order to support the delivery of the Services identified in the Order. Customer will comply with the third-party vendor-licensing terms and conditions applicable to the software package.

d) Provide Provider with the necessary connectivity and access to Customer's environment to provide the Services. Customer acknowledges that the provision of the Services is contingent upon such access.

e) Be responsible for the security, quality and integrity of source data transmitted and stored using the Services.

f) Provide Provider with reasonable advance notice of anticipated changes to Occupied Data and Protected Instance(s) more than the change rate identified in the CDR form.

g) Comply with Provider's Change Management and Notification Policy, and any other applicable Provider policies, all of which are in the Customer Portal, together with any related configuration changes to Customer's source environment (such as patches applied, upgrade of software, changes in IP address, etc.).

4. SOFTWARE AND DOCUMENTATION

The Software and Documentation are copyrighted and licensed (not sold) to Provider to provide the Services. Customer is given access to the use of the Software (in object code form only) and Documentation by Provider for the sole purpose of receiving the Services subject to the provisions of these terms and the applicable Order. Neither title nor license to the Software and/or its associated Documentation is transferred to Customer.

All Intellectual Property Rights in the Software and/or its associated Documentation subsist in Provider and/or its licensor. The Agreement does not grant Customer any right, title or interest in any Intellectual Property Rights subsisting in the Software and/or Documentation.

Customer will not delete or in any manner alter any Intellectual Property Right notices appearing on the Software and/or Documentation. Customer will reproduce such notices on all copies it makes of the Software. No license to use such notices is granted by Provider under the Agreement or otherwise, and Customer shall not use the same without Provider's prior written consent.

Customer will not:

a) Copy (except as expressly permitted by these provisions) and/or modify the Software or Documentation (in whole or part).

b) Disassemble or decompile the Software, or otherwise inspect or manipulate the Software's source code.

c) Use the Software or Documentation other than to receive the Services.

d) Lease, sublicense, transfer or otherwise distribute the Software and/or Documentation to any third party.

e) Use the Software and/or Documentation to provide service bureau, time-sharing or other computer services to third parties.

f) Install the Software on the servers or equipment of third parties.

g) Remove the Software from the Source Location without Provider's prior written consent.

h) Otherwise provide or make the Software's functionality available to third parties.

i) Otherwise cause or permit the breach of these provisions relating to Software or Documentation by a third party.

Customer acknowledges that the Software or parts of it (e.g., encryption software) and/or Documentation may be subject to in-country export controls from time to time. Customer shall not use any of them in breach of such controls.

At Provider's request and at Customer's cost and expense, Customer will provide to Provider a certificate signed by an officer of Customer verifying that the Software and its associated Documentation is being used by it in accordance with the terms of this Agreement.

On at least twenty (20) days prior written notice, Provider and/or its licensor may audit Customer's use of the Software and its associated Documentation to ensure that Customer is in compliance with the terms of this Agreement. Any such audit will be conducted during regular business hours and will not unreasonably interfere with Customer's business activities.

On termination or expiry of the applicable Order:

a) Customer's right to access and use the Software, Documentation and any Provider Confidential Information will terminate automatically.

b) Customer will destroy or return (at Provider's option) all copies of the Software, Documentation and Provider Confidential Information to Provider within fourteen (14) days.

c) An officer of Customer will certify in writing that no such Documentation, information or material have been retained or copied by Customer.

Customer acknowledges that Provider is not the developer of any of the Software and agrees that Provider shall not be responsible for any failure of or defect in the Software unless it is caused by Provider's negligence or willful misconduct.

Customer warrants that it has all necessary licenses and authorization, and consents to allow Provider to carry out the Services. Customer shall indemnify and keep Provider fully and effectively indemnified on demand against any liability, damage, expense, claim or cost (including reasonable legal costs and expenses) arising from its failure to have in place such licenses, authorization and consent.

5. CHARGES

DRaaS — Azure Service Usage charges are determined through Azure usage billing for the Azure Infrastructure Services associated with Customer's environment on a per-account basis. Azure contracted monthly usage estimate is generated from the Azure Simple Monthly Calculator tool available on the Azure public website.

Customer's use of Azure is billed monthly, in arrears. Customer will pay the total charges for the Azure Infrastructure Services. If Customer's Azure Infrastructure Services' Usage exceeds the total committed, contracted estimate amount as set out in the revenue commitment agreement, overage fees will be assessed for consumed Azure Infrastructure Services.

Customer will be assessed overages identified in the Order or, in the absence thereof, at the then-applicable rates for time and materials for the Azure usage occupied more than the number of protected virtual servers more than the Protected Instances as specified in the Order, and for the number of Tests more than the contracted Tests as specified in the Order.

Customer will be invoiced by Provider monthly for Usage-based fees for all Azure-provided services and resources consumed and used by Customer in connection with the Services for day-to-day usage as well as resources consumed during scheduled test or an actual event. These resources will be billed at the then-prevailing list rates for Azure services and resources. These Azure services and resources include, but are not limited to, the following: Zerto Cloud Appliance (ZCA) Instance, Virtual Network, VPN Gateway, Azure DNS, Azure Blob Storage, bandwidth and other similar Azure services and resources.

Customer will be billed for any Azure Infrastructure Usage from the date of Azure consumption, including during the implementation phase required for all internal and Customer testing.

The onboarding one-time fee will be billed to Customer at the Start Date of the Order. The monthly management fees per recovered server also will be billed to Customer at the Start Date of the Order in accordance with the terms set out in the Order. Overage fees will be applied to the monthly management fee if additional servers have been added.

6. MANAGED RECOVERY – AZURE GENERAL TERMS

Customer acknowledges that it is the primary processor and controller of all its data, is solely responsible for the content of all Customer data and will secure and maintain all rights in Customer data necessary for Provider and Microsoft to provide the Services to Customer without violating the rights of any third party, or otherwise obligating Provider or Microsoft to Customer or to any third party. Where applicable, Customer can select which Microsoft region its data will be located. Provider will not move Customer data into another region without Customer's consent, unless required to do so by law or by request of government agency. Customer warrants that it will process all user data (including Customer Personal Information in accordance with all applicable laws. Customer acknowledges that it is responsible for informing and obtaining consent from its users regarding the processing of their data. Customer is responsible for ensuring that it requests for Provider to take the appropriate action to secure, protect and back up its accounts and content/data in a manner that will provide appropriate security and protection, which might include use of encryption to protect its content/data from unauthorized access and routine archiving of the same. Customer acknowledges that any Services provided pursuant to these terms are strictly subject to the availability of the same from Microsoft and that any Services and service level agreements relating thereto may be subject to change, suspension, or cancellation by Microsoft. This includes the termination or suspension of the Order and Customer's Services immediately if Microsoft or Provider determines Customer is in breach of its obligations under these terms, the Agreement, or any Microsoft policies or terms referenced herein if such termination is necessary to comply with law, a security or intellectual property issue, or if Microsoft no longer permits resale of any service. Provider shall endeavor to give as much prior notice of any change or cancellation of Microsoft Service as is provided by Microsoft. Customer acknowledges and agrees that Provider shall have no liability for a failure to provide the Services or any part thereof where such failure relates to a change or discontinuance by Microsoft.

As part of its continuing commitment to improve and evolve its Services, Provider may periodically make changes, in its reasonable commercial judgment, including, but not limited to, changes to the configuration or equipment comprising the Services or discontinuing part or all of the Services provided that Provider shall notify Customer of any material change to, or discontinuation of, such Services via electronic mail or written notice to Customer's address at least thirty (30) days in advance. If any such change substantially and adversely affects Customer's ability to use the Services, Customer may, within thirty (30) days of Provider's notice to it, terminate the Order with respect to the affected Services by written notice.

BY ENTERING INTO THE ORDER, CUSTOMER ACKNOWLEDGES THAT PROVIDER IS SUBSCRIBING TO THE INFRASTRUCTURE SERVICES PURELY FOR AND ON BEHALF OF THE CUSTOMER, ACTING IN ITS CAPACITY AS RESELLER (AS SUCH IS DEFINED IN THE MICROSOFT CLOUD AGREEMENT) OF THE SAME. THE INFRASTRUCTURE SERVICES AND CUSTOMER'S USE THEREOF ARE STRICTLY SUBJECT TO THE MICROSOFT CLOUD AGREEMENT. CUSTOMER REPRESENTS AND WARRANTS THAT IT AND ITS FINANCIAL INSTITUTIONS, OR ANY PARTY THAT OWNS OR CONTROLS CUSTOMER OR ITS FINANCIAL INSTITUTIONS, ARE NOT SUBJECT TO SANCTIONS OR OTHERWISE DESIGNATED ON ANY LIST OF PROHIBITED OR RESTRICTED PARTIES, INCLUDING, BUT NOT LIMITED TO, THE LISTS MAINTAINED BY THE UNITED NATIONS SECURITY COUNCIL AND THE U.S. GOVERNMENT (E.G., THE SPECIALLY DESIGNATED NATIONALS LIST AND FOREIGN SANCTIONS EVADERS LIST OF THE U.S. DEPARTMENT OF TREASURY, AND THE ENTITY LIST OF THE U.S. DEPARTMENT OF COMMERCE). CUSTOMER IS PROHIBITED FROM RESELLING THE INFRASTRUCTURE SERVICES, OR FROM SELLING, TRANSFERRING OR SUBLICENSING CUSTOMER'S Provider OR MICROSOFT ACCOUNT CREDENTIALS TO ANY OTHER PARTY (SAVE TO AGENTS AND SUBCONTRACTORS PERFORMING WORK ON CUSTOMER'S BEHALF). NOTWITHSTANDING ANYTHING STATED TO THE CONTRARY IN THE AGREEMENT

(OR ELSEWHERE IN THE ORDER) WITH RESPECT TO: ORDER OF PRECEDENCE, LIMITATIONS OF LIABILITIES OR WARRANTIES AND THEIR DISCLAIMERS, THE PARTIES AGREE THAT THE FOLLOWING TERMS SHALL PREVAIL AND APPLY TO THE SERVICES SET OUT HEREIN: CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT, OTHER THAN THOSE WARRANTIES AND REPRESENTATIONS MADE BY MICROSOFT IN THE MICROSOFT CLOUD AGREEMENT (AND DOCUMENTS REFERRED TO THEREIN) SHALL BE THE SOLE WARRANTIES OR REPRESENTATIONS IN RELATION TO THE INFRASTRUCTURE SERVICES. CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ANY UNAVAILABILITY, NON-PERFORMANCE OR OTHER FAILURE BY MICROSOFT TO PROVIDE THE INFRASTRUCTURE SERVICES IS THE RECEIPT OF A CREDIT PURSUANT TO THE TERMS OF THE RELEVANT MICROSOFT SERVICE-LEVEL AGREEMENTS AS SET OUT IN THE SERVICELEVEL SECTION BELOW. ACCORDINGLY, Provider MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE AS TO THE INFRASTRUCTURE SERVICES, INCLUDING ANY WARRANTY THAT THE SERVICES OR THIRD-PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY MATERIALS, INCLUDING CUSTOMER MATERIALS OR THE THIRDPARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, Provider WILL NOT BE LIABLE TO CUSTOMER, AND CUSTOMER RELEASES Provider FROM ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE OR DATA) AS A RESULT OF THE USE OF THE INFRASTRUCTURE SERVICES, MICROSOFT'S PROVISION, MANAGEMENT OR OPERATION OF THE INFRASTRUCTURE SERVICES OR MICROSOFT'S EXERCISE OF ITS RIGHTS IN THE MICROSOFT CLOUD AGREEMENT OR CUSTOMER'S BREACH THEREOF, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. SERVICE-LEVEL AGREEMENTS

Provider will recover the most-recent copy of Customer's Protected Virtual Servers (OS only) for the scope defined in the Order, within the time frame set forth below following the commencement of an Event or Recovery Test. During implementation, Customer workload application dependencies will be defined and agreed with Customer. If during implementation multiple boot order recovery groups and priorities within a group are required by Customer, they will be added to the Customer Recovery Plan. Any service-level agreement (SLA) for the Service shall be subject to completion of a Recovery Plan following commencement of the Order.

Quantity of Protected Servers	On-Demand RTO (in Hours)[1]
≤ 100	2
>100	1-hour RTO to be added to 2-hours RTO for every additional 100 Servers to be recovered

If Provider fails to meet the agreed-upon or achieved RTO, Customer is entitled to a credit equal to ten percent (10%) of the Monthly Fee charged by Provider for contracted DRaaS — Azure Services for the number of managed Protected Instances listed in the Order for the month in which the failure occurred, up to maximum of one (1) month's protected server management fee. Notwithstanding the termination right described in the *General Service Terms* below, Customer may terminate the Order if Provider fails to meet the RTO SLA two (2) times within any 12-month period by providing Provider advance written notice no later than sixty (60) days following the second SLA failure.

All end-of-support components deemed to be end-of-vendor-support by Provider that Customer continues to be protected by this Service are out of scope of the above SLA. Provider will not be responsible for supporting any end of support components and will only assist Customer on a commercially reasonable basis, assuming it is still possible to do so on the Azure platform.

[1] Provider's RTO means it shall recover ATOT and ATOD all servers within the timescales set out in Customer's Recovery Plan, including the availability of the recovered server and its OS ready for Customer to access. This RTO is applicable for only latest point-in-time copy. This RTO is not applicable for cyber incident recovery as it may require iterative recoveries from one or more recovery point objectives (RPO) based nature of infection and outcome of forensic analysis (performed by customer).

8. INCIDENT RESOLUTION SERVICES

Incident Resolution Services shall be provided for those devices or Services specified in the Order as covered by Managed Services.

Where Provider detects a problem with an eligible system, Provider will notify Customer's nominated personnel (as previously notified to Provider in writing by Customer for this purpose) of the problem.

Depending upon the categorization of the problem associated with the eligible device, then within the corresponding timescale to respond from Provider's detection or having been notified by Customer of the problem, Provider will engage its then-available technical support personnel to assist (in conjunction with Customer's personnel) in problem diagnosis. Customer shall also, as soon as reasonably possible, make available its personnel to assist in problem diagnosis.

Provider does not give any guarantee or warranty, nor is it a condition of the Agreement that Provider fix any detected or notified problem with any eligible device within any timescale, as resolution will depend upon the nature and circumstances of the problem, Customer's timely assistance and response times from equipment and Software vendors. However, Provider will use its reasonable endeavors to fix the problem as soon as possible and will otherwise liaise with the equipment and Software vendors, Customer, and Customer's suppliers to enable them to do so. Furthermore, until resolution of the problem, Provider will escalate the problem internally in accordance with the escalation time flow procedures. Customer shall be responsible to pay Provider's charges in relation to provision of any additional equipment or Software, any charges or costs levied by maintenance, or Software or equipment vendors that are engaged by Provider to remedy the problem.

9. GENERAL SERVICE TERMS

ORDER OF PRECEDENCE

Notwithstanding anything to the contrary in the Agreement, if there is a conflict between these service terms and the terms of the Agreement, these service terms shall take precedence with regard to the Services provided under the applicable Order.

GENERAL POLICIES

The Services shall, at all times, be used in compliance with Provider's then-current general policies and guidelines ("Policies"). Customer agrees to be bound by the

Policies, as amended from time to time. Notices of changes to the Policies will be communicated to Customer via electronic means.

SERVICE-LEVEL AGREEMENTS; GENERAL

If Provider fails to meet the same SLA three (3) times within any 12-month period, Customer may terminate the Order by providing Provider advance written notice no later than 60 days following the third SLA failure. All virtual machine (VM) and Application Availability SLA calculations are based on a calendar month period. If Provider fails to meet an SLA, Customer is entitled to receive the applicable credit as Customer's sole monetary remedy. In no event will the total credits for all occurrences during a month exceed the Order's then-current Monthly Fee. Credits and termination rights accrue solely with respect to the root or primary SLA failure and not for SLA failures that occur as a result of a root or primary SLA failure.

Provider will not be responsible for the failure to meet an SLA if the failure is caused by:

a) A breach of the Agreement by Customer, its employees, subcontractors or agents ("Customer Representatives").

b) The negligence or intentional acts or omissions of Customer or Customer Representatives (including Customer retention of root or admin access and changes to data or configurations).

c) Customer requiring Provider to continue to maintain or use unsupported software or hardware releases, scheduled or emergency maintenance (including upgrades, repair or component replacement or scheduled backups) or other mutually agreed-to downtime.

d) Scheduled maintenance on Provider's shared infrastructure, applications and platforms ("Lifecycle Maintenance"). Lifecycle Maintenance currently is scheduled every third Sunday between the hours of 1AM and 6AM (local time), and no further notice to Customer is required. If Provider changes its Lifecycle Maintenance window, Provider will provide Customer with 30-day advance notice.

e) The absence of a patch, repair, policy, configuration or maintenance change recommended by Provider, but not approved by Customer; or configurations or architectures that are not supported or recommended by the applicable vendor.

g) Failure of the Customer's software or hardware, except where Provider is responsible under the applicable Order for the management or operation of the same, or where such failure results from a breach by Provider of its obligations under the applicable Order.