Schedule

Disaster Recovery as a Services

This Schedule sets out the additional terms and conditions applicable to the Customer's use of the Rogers Disaster Recovery as a Service (the "Services"), details of which are stipulated in the Product Quotation. This Schedule is an attachment to and forms an integral part of the Customer's Master Enterprise Customer Agreement (the "Agreement") with Rogers. The Customer agrees to be bound by the terms and conditions set out in the Agreement, which include without limitation this attachment and any other attachments to the Agreement. Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Agreement.

1. **Definitions:**

1.1. "Availability" — In calculating whether or not Rogers has met the commitments in any specific Calendar Month the lack of Compute Availability owing to downtime for any of the reasons set out below will not be factored into the SLA calculations: Scheduled Maintenance; Emergency Maintenance; Customer's failure to comply with its obligations as defined in the Agreement, including failure to pay valid past-due amounts or any suspension of the Services due to Customer's credit worthiness; failures of the Customer's applications or any Customer equipment not within the sole control of Rogers or a party under contract with Rogers to provide services in connection with the Agreement and/or the Product Schedule; acts or omissions of Customer or any use or user of Disaster Recovery as a Service authorized by Customer and, or during an event of Force Majeure.

1.2. "Calendar Month" — a period from a specified day in one month to the day numerically corresponding to that day in the following month, less one;

1.3. "Corporate Support Team" — Corporate Support Team means the technical support group at Rogers' responsible for handling all support requests from Customers. The Corporate Support Team operates 24x7x365. The support is provided from Canada, excluding any technical action which may be handled remotely from outside of Canada. Support is available in English and French.

1.4. "Disaster Recovery Secondary Site Availability" — For each customer Organization, Rogers will use its Platform Monitoring and Alarming system to poll the availability of each type of storage. Compute means the vCPU and vRAM resources available for Customers to use made available to the Customer from within vCloud Director.

1.5. "Emergency Maintenance" — Emergency Maintenance means any maintenance activities performed to prevent potential failures to infrastructure on which Services are connected or avoid a security breach that could compromise Customer's Content. Where possible, and if the situation allows for it, the Customers will be notified by Rogers within twenty-four (24) hours of any such Emergency Maintenance.

1.6. "Incident Management" — An Incident means an unplanned interruption to any part of Disaster Recovery as a Service or reduction in the quality of Disaster Recovery as a Service. An Incident can be created by a Customer by using either the MyAccount portal or by contacting the Corporate Support Team, or generated by the Rogers Platform Monitoring and Alarming system. All Incidents will be assigned an identification number in the Rogers Support System to be used for tracking and record keeping.

1.7. "Incident Management Resolution" — Incident Management Resolution means that the service has been restored as per the SLA and this resolution has communicated to the Customer by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.

1.8. "Method of Procedure (MOP)" — A method of procedure (MOP) is a step-by-step set of instructions for completing an operation. It tells the Managed and Professional Services operations technicians what operations to execute, and in what order.

1.9. "Move/Add/Change/Delete (MACD) Request" — MACD means Customer requests which are 'add-ons', changes or compliment of Disaster Recovery as a Service. These are requests which are not in scope to be handled as part of the subscribed service by the Corporate Support Team. Such requests require additional billable fees and a sales order to implement. Deletions are removals of a partial 'add-on' or primary service, which result in a change of billing or service.

1.10. "Organization" — Within the vCloud Director, Customers can build logical organizations. These include Users & Policies, Organizational Virtual Datacentres, and Catalogs (images and templates). Each organization can be attached to one or more Virtual Datacentres.

1.11. "Primary Site" — Primary Site means the location(s) in which the customer is responsible for the data centre and compute resources or Rogers through another agreement.

1.12. "Platform Monitoring and Alarming" — The tools used by Rogers to determine the availability of Disaster Recovery as a Service.

1.13. "Response" — measured from the time a Customer calls or creates an Incident ticket in MyAccount Portal to the time a Rogers employee updates the ticket, speaks to, chats, or emails the customer.

1.14. "Rogers Support System" — The tools used by Rogers to record and track all Service Requests and Incidents Requests as part of Disaster Recovery as a Service.

1.15. "Scheduled Maintenance" — Scheduled Maintenance means any maintenance activities performed on the infrastructure to which Customer's Services are connected. Customer shall be given at least five (5) days advance notice of Scheduled maintenance activities. The details of the service window and the Customers' negative impact will be communicated to the Customer in the notification.

1.16. "Secondary Site" — Secondary Site or Rogers Hosted Secondary Site means the physical location, including the data center and compute resources made available by Rogers to the Customer in the event of a disaster event.

1.17. "Self-Service" — Self Service means any operation carried out by the Customer using an available tool provided by Rogers without submitting a ticket or contacting the Corporate Support Team.

1.18. "Service Request" — Service Request means a request from the Customer to the Corporate Support Team for information, or advice, or for a standard change not related to an Incident or a MACD. A Service Request can be created by a Customer through the MyAccount portal or by contacting the Corporate Support Team. All Service Requests will be assigned an identification number in the Rogers Support System to be used for tracking and record keeping.

1.19. "Service Request Resolution" — Service Request Resolution means that the Service Request has been completed and Rogers has communicated this to the Customer by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.

2. **Features.** Disaster Recovery as Service ("**Service**") includes a combination of site failover test and orchestration software, reserved compute (CPU/RAM) units and storage, and a virtualization environment. The Service does not include Disaster Recovery consulting or Business Continuity consulting, which may be purchased separately from Rogers and the conditions for such services will be contained in the respective Statement of Work. Disaster Recovery as a Service consists of the following components:

2.1. **Primary Site.** This is the source site for all the customer content to be protected as part of the Rogers Disaster Recovery as a Service. For the purposes of describing the Rogers Disaster Recovery as a Service, any site that is not the Rogers Secondary Failover Site will be considered a Primary Site.

2.2. **Secondary Failover Site.** This is the Rogers hosted target for customer data protected as part of the Rogers Disaster Recovery as a Service. The customer's content will be copied to this site. This is the location that the customer will use to restore their content to a working state during a disaster or failover test.

2.3. **Zerto Virtual Manager (ZVM).** A software plugin for the Customer's primary virtualized environment's hypervisor. Responsible for replicating virtual machines from the primary site to the Rogers hosted secondary site as well as tracking and managing failover and failback states for the entire environment.

2.4. **Zerto Replication Appliance (VRA).** Software installed into a virtual machine running within the Customer's primary virtualized environment responsible for tracking and managing replication between the Customer's primary site and the Rogers hosted secondary site.

2.5. **Zerto User Interface.** A GUI used by the Customer to configure, test, and manage the disaster recovery solution, including orchestration of disaster recovery testing and production failover and failback

2.6. **Zerto Replication Host License (per VM).** A license is required for each Virtual Machine instance that is part of the Disaster Recovery Solution. The license enables a virtual machine at the Customer primary location to participate in the Disaster Recovery as a Service replication and failover orchestration.

2.7. **Zerto Replication Compute Unit.** A computing resource pool in the Rogers hosted secondary site. A Compute Unit is a fixed ratio of vCPU to vRAM. The ratio for the Services is 1vCPU:2GB vRAM.

2.8. **Zerto Post-Disaster Utilization.** Utilization of Zerto Replication calculated by the number of used GB of vRAM per hour in the Rogers hosted secondary site during a disaster recovery event

2.9. **Zerto Post-Disaster Windows OS Usage.** Hourly utilization of virtual machine instances running Microsoft Windows Server

2.10. **MyAccount Portal.** The Rogers portal that Customers use to manage their user accounts, review billing information, open and review support tickets, purchase additional Services, and review their reporting.

2.11. **Zerto Replication Storage.** Reserved storage resources at the Rogers secondary site supporting the replication of Customer's virtual machines.

2.12. **Network.** Internet connectivity or supporting cross connect services at the Rogers hosted secondary site in support of customer data replication and access to the Rogers hosted environment during a Disaster Recopy event.

2.13. **VMware vSphere.** The virtualized environment on which a Customer's Services run is VMware ESXi.

2.14. **VMware vCloud Director.** The VMware portal that presents the Services to the Customer to self-administer. The vCloud Director is the primary tool that Customers will use to access the post failover Services.

2.15. **Platform Management Monitoring and Alarming.** The hosted infrastructure at the secondary disaster recovery site is managed by Rogers. Rogers will manage and monitor the physical hosts, switching, storage, and hypervisor components; threshold alerting (Configuration of alerts based on sustained capacity usage and industry standards), quarterly reports (usage reports CPU, RAM, Drives, Uptime, trending, capacity planning), hardware inventory management (hardware inventory reports), Issue identification and remediation; and SLA statistics.

2.16. **Infrastructure Refresh.** All equipment manufacturer guarantees, warranties and service agreements are purchased by Rogers and maintained by Rogers. Rogers will refresh the equipment (the "**Rogers Equipment**") as needed to support the Services.

2.17. **Professional Services.** The design, implementation, and handover of the Disaster Recovery as a Service solution to the customer required Rogers Professional Services. This work and supporting quote to the Customer is provided in a separate Statement of Work. Professional Services is required for all sales of the Service.

2.18. **MS Assisted Disaster Recovery as a Service ("MS Assisted DRaaS") (optional).** Optionally, Customer may purchase an add-on service, the "MS Assisted DRaaS". In addition to the Professional Services team's assistance, the RDC Managed Service team will provide assistance related to the planning, testing and management of Customers' recovery strategy. A completed SOW in the form provided by Rogers and including the details of the services must be completed in writing by Customer and returned to Rogers in order to obtain such services, as well as an expedited MOP support request, if needed. An active Managed Service is required on servers/systems and software for the MOP instructions to be performed (i.e.: RDC Managed Server, RDC Managed Firewall, RDC Managed Router, RDC Managed Switch).

3. **User Subscription types (Standard and Principal).** Access to the Services is configured for two (2) types of users as set out below. The Customer's account will specify the user type. The two available user types are:

i) **Standard User** – this user level gives a single user the right to access the Disaster Recovery Service and the additional privileges/responsibilities below.

a) Access the Zerto User Interface

b) Initiate and Managed a Disaster Recovery test

c) Initiate and manage a disaster recovery event, including failover and failback orchestration

ii) **Principal User** – this user level gives a single user the right to access the Disaster Recovery Service as well as the additional privileges/responsibilities below:

a) Purchasing additional services through the "Buy More" function:

b) Responsible for keeping the account information up to date;

c) Responsible for providing current Customer contact information for Rogers automatic notification systems;

d) Responsible for receiving all notices from Rogers relating to the Services.

4. **Customer Responsibilities and Acceptable Use Policy:**

i) Customer is solely responsible for the creation, management, testing, and execution of their business continuity & disaster recovery plan. The customer is responsible for declaring a disaster recovery event and ensuring that their technical staff is able to execute on their business continuity & disaster recovery plan using Disaster Recovery as a Service.

ii) Customer is responsible for configuring, managing, monitoring, and maintaining their primary site's infrastructure, network, software licenses, and applications.

iii) Customer must grant a Rogers technician or Rogers authorized agent administrator level access to their primary site's virtualized environment, including hypervisor level access in support of the initial installation, configuration, and testing of Disaster Recovery as a Service. Administrative level access will also be granted upon Rogers request in support of service trouble shooting and support. Reduced permissions post installation can be discussed with Rogers Professional Services.

iv) Customer must ensure that their hypervisor and its associated version is compatible with the version required by Rogers for the Services. Rogers will publish a list of supported hypervisors and version along with notification to the Customer of any support changes as part of Rogers Change Management process. Rogers is not responsible for providing, or for any cost or expenses associated with providing, any administrative, configuration, technical, emergency or support personnel associated with the restoration, upgrading, or changes or restoration of the Rogers Disaster Recovery as a Service due to the Customer performing any changes to their own Primary Site environment or software.

v) Customer will not attempt to use the Rogers Failover Site infrastructure as their permanent production site for more than 3 months without contacting Rogers Support. Rogers Support may suggest alternative solutions for the customer and will work to create a long term plan that may require other Rogers Services be added or substituted.

vi) Customer will notify Rogers of any changes to their primary site's configuration and environment, including but not limited to: addition, removing, or changes to virtual machines, any changes to software licensing EULA, network configurations, software and hypervisor upgrades or changes, hardware upgrades or changes including network, server, and storage.

vii) Customer bears all risk associated with its use of the Services.

viii) Customer is responsible to ensure that the Services are sufficient for its needs.

ix) Customer is solely responsible to determine that its use of the Services is compliant with all laws and regulations applicable to the Customer.

x) Customer agrees to use the Services in compliance with all applicable laws and regulations, including, without limitation applicable privacy laws.

xi) Customer agrees not to use the Services:

a) To violate or infringe on the rights of other customers;

b) To use the Services to gain unauthorized access to or to disrupt in any manner any third-party service, device, data account or network;

c) To spam or distribute malware;

d) In any way that could harm the Services or impair other's users use of the Services;

e) In any manner where failure of such a use could lead to serious injury or death to any person or to severe physical or environmental damage.

xii) To the extent required by applicable laws and Customer's own business requirements, the Customer shall retain connection logs, or any data required to identify any internal or other user of the Customer's own services hosted on the Services.

xiii) Customer shall not use the Services to deploy services which are intended to enable users to download files to and from file hosting platforms including but not limited to BitTorrent etc.

xiv) Customer is solely responsible for use of the Services by any individual to whom the Customer may have provided its password(s) and any other means of access (such as SSH access keys, API, etc.).

xv) Customer is solely liable for the consequences of the loss of any passwords and any other means of access to the Services.

xvi) Customer is responsible for providing appropriate staff to participate in troubleshooting incidents and service requests. During an incident or a service request the Customer will actively participate in the resolution of the request. Any time spent waiting for communications from the Customer may result in the severity of the ticket getting downgraded and the time subtracted from the resolution time.

xvii) Customer is responsible for coordinating all communications with any third party they have contracted to provide any type of support for their services

xviii) Customer is responsible for maintaining strong password to access the Services. Changes to the access controls require the provision of a Customer designated secure user name and password. Credentials designated by the Customer must utilize strong security traits (e.g. upper and lower case values, numeric and non-numeric values). Customer is responsible for credentials and must keep credentials secure and confidential.

xix) Customer shall be solely responsible for providing the Customer's services, technical support, pricing and service plans, billing and collections, and any and all other services to the Customer's end users, and Rogers shall have no obligations or liability whatsoever to end users in relation to Disaster Recovery as a Service.

xx) Customer will inform all users of any terms and conditions and any associated costs including any potential charges, overages, and other fees associated with the Services. The Customer agrees to pay any such charges based on use of the Services by their end users.

xxi) In addition to the indemnification provisions set out in the Agreement Customer shall defend and indemnify Rogers, its parents, successors, Affiliates and agents from any claims, damages, losses or expenses (including without limitation legal fees and costs) incurred by Rogers in connection with all claims, suits, judgements, and causes of action (i) for any third party intellectual property rights, for which the Customer agrees to lawfully obtain any licenses required, if any, to use any third-party intellectual property, including software; (ii) the use of any third-party licenses including but not limited to, Microsoft, Red Hat, and Oracle, ; (iii) and any third-party content.

xxii) Violation of the terms in this section may result in suspension of the Service. Rogers may, at its sole discretion suspend the Service only to the extent reasonably necessary.

xxiii) Unless Rogers believes an immediate suspension of a Customer's Services is required, Rogers will use reasonable efforts to provide notice before suspending a Customer's Services.

xxiv) The Services will continue on a month to month basis after the end of the Term with the following conditions:

a) The Customer is responsible for making end of the Term arrangements by renewing their Services or cancelling the Services.

b) If the Customer does not make end of Term arrangements, then Rogers may, in its sole discretion, terminate the Services.

5. **Customer Indemnity.** In addition to the indemnification provisions set out in the Agreement, the Customer shall defend and indemnify Rogers, its parents, successors, Affiliates and agents from any claims, damages, losses or expenses (including without limitation legal fees and costs) incurred by Rogers in connection with all claims, suits, judgements, and causes of action (i) for any third party intellectual property rights, for which the Customer agrees to lawfully obtain any licences required, if any, to use any third-party intellectual property, including software; (ii) the use of any third-party licenses including but not limited to, Microsoft, Red Hat, and Oracle, ; (iii) and any third-party content.

6. **Rates and Charges.**

i) The term of each Disaster Recovery as a Service (each an "**Initial Service Term**") is as set forth in the Product Quotation(s). The term of this Schedule commences on the date of signature of the Agreement by Customer, or, if this Schedule is attached to the Agreement by way of amendment, then on the date of signature of said amendment by Customer. Upon expiration of the Initial Service Term, a Disaster Recovery as a Service may be renewed for an additional period set forth in a Product Quotation to be added to this Agreement by way of amendment (a "**Renewal Service Term**") or, if no amendment is executed, the Disaster Recovery as a Service will automatically renew on a month-to-month basis (a "**Month-to-Month Renewal Term**"). The Initial Service Term, Renewal Service Term and Month-to-Month Renewal Term" are collectively referred to as a "**Service Term**".

ii) The Fees for the Disaster Recovery as a Service, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Product Quotation(s). Professional service charges are set out in any applicable Statement of Work. Customer is solely responsible in the event of charges arising from fraudulent and/or unauthorized use of Customer equipment, Rogers' equipment or Disaster Recovery as a Service by any third party or unauthorized person.

iii) Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Monthly Recurring Charges set out in any applicable Product Quotation represent minimum charges. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.

iv) During a disaster recovery event, consumption of post-disaster recovery components will be metered based on the duration of the failover event, rounded up to the nearest hour. The hourly charges for post disaster recovery components is set out in the Product Quote.

v) Unless otherwise agreed to in writing by Rogers and Customer, Rogers reserves the right to commence billing Customer for the Disaster Recovery as a Service on the earlier of thirty (30) days following execution by the Customer of the Agreement related to the Disaster Recovery as a Service or thirty (30) days after the Service Effective Date in accordance with this Schedule. Rogers will, by way of invoice or otherwise, notify you of the Service Effective Date. In the first month, the charges will be prorated for the number of days in the month after the billing commencement date. Applicable Service Credits will be applied to Customer's invoice within two billing cycles after Rogers approves Customer's request for Service Credits.

vi) If the Customer purchases additional services through a web-portal provided by Rogers for that purpose ("**Buy More**"), the rates for the Services will increase accordingly and any such additional services will be co-terminus with the Term for the Services.

vii) Rogers reserves the right to change rates for any and all Disaster Recovery as a Service throughout the Service Term upon the provision of ninety (90) days' written notice to Customer in the event of an increase in third party supplier costs.

viii) Upon the commencement of a Month-to-Month Renewal Term for a Disaster Recovery as a Service, the rates for such Disaster Recovery as a Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.

ix) Customer must pay invoices within thirty (30) days of the date of each Rogers invoice.

7. **Backup, Content Integrity and Disaster Recovery.**

i) Rogers is not responsible for providing, or for any cost or expenses associated with providing, any administrative, technical, emergency or support personnel associated with Backup Software for providing and maintaining the Customer Content (defined below) unless otherwise contracted.

ii) Notwithstanding anything to the contrary, the Services do not backup Customer Content as part of the Services. The Customer agrees to take all the necessary measures to back up their Content in the event of data loss/Content loss or deterioration of Customer Content, whatever the cause.

iii) For greater certainty, the inclusion of data replication (as part of resiliency) shall not be considered "data backup" for the purposes hereof.

iv) The Customer is solely responsible to set up their own business continuity plan and/or business recovery plan.

8. **Services and Networking.**

8.1. **Disaster Recovery Testing:** The services include 48 hours per calendar year of disaster recovery testing. Utilization of the Services for testing purposes in excess of 48 hours will be charged based on the Post-Disaster service components set out in the Product Quote.

8.2. **Network Access:** The Services include access to a shared internet connection with a maximum throughput of 250Mbps. Customers will access the Services by way of this shared internet connection. If a Customer requires private or dedicated network access, they can purchase a Rogers Wireline service.

8.3. **Data Centre Carrier Neutrality:** Rogers will, in its sole discretion, allow third party network and access providers to provide connectivity to the Customer's Disaster Recovery Service. Rogers will provision the cross-connection between the Customer's colocation space and the third party connectivity provider. The Customer is responsible for all charges for cross-connection supplied by Rogers. Rogers will not provide support, guarantee performance, be responsible, or make any representations or warranties for such third party connectivity services.

8.4. **Ownership of the Service:** The Customer will under no circumstances be permitted to access the physical space or the surrounding facility from which the Services are performed. The Customer will not acquire any interest in, nor file any liens upon, the Data Centre, the Rogers Equipment, and any portion of the data centre as a result of the provision by Rogers of the Service or their termination for any reason pursuant to the Agreement.

8.5. **Fair Use of the Services:** The Services are subject to fair use by Rogers Customers. Rogers will ensure that Customers do not disrupt the use of other users of the Services. Rogers will prevent Noisy Neighbours and will generally limit the ability of Customers to adversely affect other users and other Customers. Noisy Neighbor means a Customer and/or a user that monopolizes bandwidth, disk I/O, CPU and other resources, and may negatively affect other users' cloud performance. If Rogers, in its sole discretion determines that a Customer is a Noisy Neighbour Rogers may, and Rogers reserves the right to temporarily limit a Customer's use of the Services. Rogers will attempt to contact the Customer prior to any corrective action. Any action by Rogers to address a Noisy Neighbour and any disruption to the Customer's Services is excluded from the SLA for the Services.

8.6. **Client Side Internet:** The Customer will access the Services remotely via the internet. The Customer must have their own local internet connection to access the Service, and is solely responsible for the aforementioned internet connection, in particular its availability, reliability and security unless otherwise contracted by Rogers.

8.7. **Measures for the prevention of spamming:** The Customer is prohibited from using the Services for spamming, for any intrusive activity or any intrusion attempt from the Service (including, but not limited to: port scans, sniffing, spoofing), and any activity or contentious behaviour such as traffic exchanging (Hitleap, Jingling), Black Hat SEO (downloading and uploading videos from and to online gaming platforms), crypto-currency mining, video game bots, or other similar other prohibited or abusive activities. In such cases, Rogers may cease providing and terminate access to the Services immediately. Rogers may implement a system of technical measures intended to prevent the dispatch of fraudulent emails and spam from the Services. Rogers may monitor outgoing traffic patterns from the Service towards port 25 (SMTP server) on the internet by means of automatic tools.

9. Security Access and Fraud.

i) The Customer agrees to implement and is wholly responsible for implementing reasonable security precautions and practices in relation to the use of Disaster Recovery as a Service.

ii) The Customer is solely responsible for any non-physical security breach or unauthorized usage of Disaster Recovery as a Service.

iii) Rogers shall limit access to Disaster Recovery as a Service and take reasonable security efforts to prevent unauthorized access to of Disaster Recovery as a Service.

iv) The Customer is solely responsible for user access security or network access security with respect to the Customer Content.

v) Rogers shall use reasonable commercial efforts to assist in network security breach detection or identification. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches and is not liable for any security breach that occurs despite its efforts.

vi) The Customer is responsible for identifying all user management rules for the account. This includes identifying which individuals have access to account administrative, security, technical and billing rights. The Customer is responsible for any use of the account regardless of who uses the Services.

vii) Rogers will track all access to the Customer's Services through the online ticketing system/support system and will ensure that they have all necessary documented Customer approvals prior to accessing or changing the Customer's Services. If Rogers cannot verify the Customer's identity or suspects that there may be fraudulent or illegal activity Rogers may decline the request. In such an event Rogers will attempt to contact the main or alternative contact or the Principal User.

viii) When a situation is considered a security breach or could have serious consequences, Rogers will notify the Customer and will act on the Customer's behalf if Rogers is unable to get correct approvals in a timely manner to deal with the threat.

ix) In the event of any emergency that presents a substantial risk of a service outage, or damage to Rogers Equipment or data belonging to Rogers, a third party, the data centre facilities, or to any persons or property present therein, Rogers shall take all reasonable measures to respond to the emergency; and only as necessary, Rogers may disable Disaster Recovery as a Service if the emergency requires such action to avoid damage.

x) The Customer agrees to co-operate and assist Rogers with any investigation or action taken in relation to Rogers' operations and provisioning of services, confirmation of Customer compliance with the Agreement and, or breach of the Agreement by the Customer.

xi) All Content within Disaster Recovery as a Service is completely isolated through the use of industry standard virtualization protocols and VLAN rules within the infrastructure. Customers are further isolated with virtual firewalls. All Content will be located within the of Disaster Recovery as a Service secondary site is housed within one of Rogers' data centre facilities located within Canada.

xii) The Customer is not permitted to run security penetration tests on Disaster Recovery as a Service without prior written approval from Rogers. Any such actions will be considered an improper use under the Agreement. Rogers may, without liability, restrict Virtual Data Centre access if Customer performs invasive platform testing without written approval.

xiii) To the extent practicable, updates are performed in collaboration with Customer. For any avoidance of doubt, after the delivery of the Service to the Customer, the responsibility to manage and update of the operating systems and pre-installed applications is transferred to the Customer.

xiv) Notwithstanding the foregoing, Rogers reserves the right to request that the Customer install updates and patches in connection to running Services. If the Customer fails to comply with the reasonable request of Rogers to update the operating system or application, and such failure to comply creates a security risk to the Customer's Content or the Services or to Rogers, its Subcontractors, or other customers, Rogers may suspend access to the Service(s) until the Customer complies with such request or the Service is reinstalled.

xv) If Rogers detects or reasonably believes that the Customer's usage represents a security risk, an email will be sent to Customer, identifying the account(s) affected, and stating that a reinstallation procedure must be performed in order to maintain the integrity of the Service and the entire infrastructure.

xvi) In case of a security breach Rogers reserves the right to suspend the Services immediately in order to maintain the integrity of the Customer's Content.

xvii) Rogers reserves the right, without incurring liability, to suspend the Services, if there is (a) a threat to the stability and/or security systems of Rogers' infrastructure, the Services and/or Customer data/Content, or (b) a Customer's breach of the Agreement. Any such suspension can occur without prior notice in the event of an emergency, including in the event described in point (a) above, or in the case of unlawful or fraudulent use of the Services, or as part of a request from a competent administrative or judicial authority. The Customer acknowledges that such suspensions do not release it of any obligation to pay for the Services.

xviii) Rogers shall not be held responsible for the Customer's usage of the Disaster Recovery as a Service, notably for any misuse of the Services by the Customer through the Self Service Portal.

10. **Support.**

i) When reporting an incident and creating a ticket for the purposes of technical support, the Customer agrees to provide Rogers with all relevant information reasonably required for the diagnosis and intervention of the incident.

ii) The Customer undertakes to remain available in order to collaborate with Rogers including by providing further information and carrying out reasonably required tests and checks. In certain circumstances, a technical support issue may require the Customer to provide Rogers access to its Service. If the Customer is not available as set forth in this section, it cannot benefit from the service level targets defined above to the extent a failure to achieve a service level target is attributable to Rogers' unavailability.

11. **Operating System (OS) & Software License Grant.** Upon purchase of Disaster Recovery as a Service by Customer, Rogers will grant to Customer licenses for the use of the service, including Zerto software as well as Microsoft Windows Service licenses for use during post-disaster. These licenses are subject to and subordinate to the underlying End User License Agreement (EULA) from the OS or Software licensor.

i) The Customer agrees they have read, understood, and agreed to the following EULA's if making use of any such services:

a) The Services described herein are subject to additional license terms, with which the Customer hereby agrees to comply. Customer's use of Microsoft software is subject to Microsoft's End User License Terms, which are set forth below. The EULA for Microsoft OS licenses is located here: https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms(WW)(ENG)(Apr2014)(CR).pdf

b) EULA for VMWare is located here: https://myaccount.datacentres.rogers.com/legal/vmware_universal_eula.pdf

c) EULA for Redhat is located here: https://myaccount.datacentres.rogers.com/legal/GLOBAL_EULA_RHEL_English_20101110.pdf

d) EULA for Zerto is located here: https://myaccount.datacentres.rogers.com/legal/ZertoEndUserLicenseAgreement.pdf

ii) Any licenses provided by Rogers to the Customer for Disaster Recovery as a Service are solely permitted for use with the Services. Upon termination of Disaster Recovery as a Service for any reason, these licenses shall be terminated, and Customer shall have no further rights to the Software, except as necessary to comply with the Agreement. For greater clarity, “Customer” in the above paragraph shall also include all end users.

iii) The Customer will have the right to provide its own non-Microsoft based OS and associated software licensing to be used with Disaster Recovery as a Service. The Customer agrees that, in the event the Customer provides its own non-Microsoft based OS and associated software licenses, the Customer has taken all necessary steps to ensure that the licenses being used are legally licensed and supported through an agreement between the Customer and the software provider. The Customer will, if required by Rogers, provide proof of purchase for all Customer-provided licensing being used with Disaster Recovery as a Service.

iv) If the Customer makes use any non-Rogers provided software, the Customer represents and warrants to Rogers that the Customer has the right and applicable license to use the software in that manner.

v) If Rogers has agreed to provide management services, then the Customer represents and warrants that the Customer’s software license agreement with the software provider permits Rogers to perform these activities.

vi) The Customer is responsible for reporting to Rogers any changes to their use of the Services including but not limited to Disaster Recovery as a Service, virtual machines, or software agreements that impact their compliance with any software EULA. If the Customer fails to disclose such changes the Customer is liable for any incremental software licensing fees incurred by Rogers from the time of the change.

12. **Content.**

12.1. **Definition of Customer Content.** Customer Content is defined as any software (including machine images), data, text, audio, and video or images that a Customer or any user transfers to Rogers for processing, storage or hosting by the Services in connection with the Customer's account and any computational results that a Customer or any user derives from the foregoing through their use of the Services.

i) Customer Content does not include account information. The terms of the Agreement or other agreement with us governing the use of Services apply to the Customer Content.

ii) Ownership of Content. All interest in and ownership of Content including, but not limited to, those portions of the Content that are Customer trade names, trademarks or service marks, are and shall remain the property of the Customer

iii) Rogers is only responsible for maintaining the environment with a level of redundancy in accordance with the Service Level Agreement set out below. This redundancy does not extend to backups of Customer Content located within Disaster Recovery as a Service.

iv) Customer shall remove all Content from Disaster Recovery as a Service at the date of termination of the Services. In the event that the Content is not removed, such Content will be considered abandoned, and Rogers may, without liability to the Customer, delete the Content.

v) When evaluating the security of a cloud solution, it is important for Customers to understand and distinguish between the following:

a) Rogers is responsible for protecting the infrastructure that runs all of the services offered as part of the Services. This infrastructure is composed of the hardware, software, networking, and facilities that run the Services.

b) Customer responsibility is determined by the services that a Customer has contracted for with Rogers. If a Customer contracts for a Rogers cloud service, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the Customer in the cloud service, and the configuration of any Rogers-provided firewall.

vi) If the Customer has contracted for managed services with Rogers please refer to such other terms.

13. **Service Level Agreement (“SLA”).** If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, Customer shall be entitled to a service level credit (“**Service Credit**”).

Table 1: Power Availability

	Monthly Objective	Objective	Service Level Credit

Disaster Recovery Second Site Availability	99.99%	Poll Disaster Recovery as a Service Gateway every 5 min. for connectivity to the Internet or Wide Area Network (WAN) and to Storage, then record a value of UP or DOWN. If the Disaster Recovery as a Service Gateway is DOWN perform the following calculation: Impact = SUM(DOWN_POLL) Deviation = Total time available in the Month in Min. – Impact Availability = Deviation / Total time available in the Month in Min. X 100	99.99% to 99.85% Monthly = Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to the Customer in an amount equal to the total monthly bill for the affected service monthly fee paid by the Customer for the affected Services.
MyAccount Portal (MyAccount API and MyAccount Web Portal)	99.99%	Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN. mpact = SUM(DOWN_POLL) Deviation = Total time available in the Calendar Month in Min. – Impact Availability = Deviation / Total time available in the Month in Min. X 100	99.99% to 99.85% Monthly = Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to the Customer in an amount equal to the total monthly bill for the affected service monthly fee paid by the Customer for the affected Services.
Zerto Service Portals (Zerto dedicated vCloud Director and Zerto Management Portal (Cloud Based))	99.99%	Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN. mpact = SUM(DOWN_POLL) Deviation = Total time available in the Calendar Month in Min. – Impact Availability = Deviation / Total time available in the Month in Min. X 100	99.99% to 99.85% Monthly = Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to the Customer in an amount equal to the total monthly bill for the affected service monthly fee paid by the Customer for the affected Services.

Table 2: Incident Management Response Time and Resolution

Severity Level	Response Time and Resolution	Objective	Service Level Credit
Incident Management – Severity 1	Response Time Target and Incident Management Resolution Target as indicated below.	Response Target Metric: When a Customer calls in live 24x7 = Live answer When a Customer creates in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Six (6) Hours	Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the cumulative duration of such unavailability during such Calendar Month.
Incident Management – Severity 2	Response Time Target and Incident Management Resolution Target as indicated below.	Response Target Metric: When a Customer calls in live 24x7 = Live answer When a Customer creates in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Fourteen (14) Hours	Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the cumulative duration of such unavailability during such Calendar Month.
Incident Management – Severity 3	Response Time Target and Incident Management Resolution Target as indicated below.	Response Target Metric: When a Customer calls in live 24x7 = Live answer When a Customer creates in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Seventy-two (72) Hours	Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the cumulative duration of such unavailability during such Calendar Month.
Service Request	Response Time Target as indicated below.	Response Target Metric: When a Customer calls in live 24x7 = Live answer	Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the

		When a Customer creates in MyAccount Portal = Two (2) hours Service Request Resolution Target: Five (5) Business Days (Monday to Friday 8am to 8pm EST)	cumulative duration of such unavailability during such Calendar Month.
MOP Service Request	Response Time Target as indicated below.	Response Target Metric: When a Customer calls in live 24x7 = Live answer When a Customer creates in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Six (6) Hours	Rogers will issue a credit to the Customer in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by the Customer of the cumulative duration of such unavailability during such Calendar Month.
Move/Add/Change/Delete (MACD) Request	Response Time Target as indicated below.	Response Target Metric: When a Customer calls in live 24x7 = Live answer When a Customer creates in MyAccount Portal = Two (2) hours MACD Request Resolution Target: Scoping performed on a case by case basis	Service Level Objective only (no Service Level Credit)

13.1. **<u>Incident Management Severity Levels (Table 2):</u>**

i) Severity 1: Critical - total or majority loss of critical service (i.e. Production server or other mission critical system(s) are down and no workaround is immediately available): All or a substantial portion of the Customer's Content is at a significant risk of loss or corruption; Customer has had a substantial loss of service; and Customer's business operations have been severely disrupted.

ii) Severity 2: Major functionality is severely impaired. High impact; and Degradation of critical service or total of loss non-critical services

iii) Severity Level 3 (S3) Partial, non-critical loss of functionality of the Services. Low impact – no direct business impact; and Non-critical services affected;

iv) Service Request: A request from the Customer to the Corporate Support Team for information, or advice, or for a standard change not related to an Incident or a MACD (Move/Add/Change/Delete).

v) Move/Add/Change/Delete (MACD) Request: Are requests which are 'add-ons' or compliment the Disaster Recovery as a Service. These are requests which are not in scope to be handled as part of the Service by the Corporate Support Team and are supported by billable fees and a sales order to implement. Deletions are removals of a partial 'add-on' or primary service, which result in a change of billing or service.

13.2. **<u>Calculation for Response Time and Resolution Target (Table 2) for Incident Management (except if SLO):</u>**

i) Response Time Target Rogers response time will be measured from the time a Customer calls or creates an Incident ticket in MyAccount Portal (Rogers Support System) to the time a Rogers employee updates the ticket in the Rogers Support System, speaks, chats, or emails the Customer.

ii) Rogers' resolution will be measured from the time a Customer calls or creates an Incident ticket in MyAccount Portal (Rogers Support System) to the time a Rogers employee updates the Rogers Support System ticket informing the Customer the incident is resolved.

iii) <u>Monthly Service Level Credit Limitation.</u> The combined cumulative total of all Service Credits for a calendar month for the Services will not exceed the total Monthly Recurring Charges for the affected Services that Rogers has invoiced for such calendar month.

iv) <u>Service Credit Request Process.</u> If Rogers has failed to meet any of the above service levels for a particular Customer Site in any given billing month, Customer must contact Rogers and apply for a Service Credit within thirty (30) days following the end of the month for which the Service Credit is sought. Upon Rogers' confirmation that the Service level was not met, Rogers shall issue a Service Credit to Customer.

v) Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are Customer's sole and exclusive remedy for any failure or interruption in the Disaster Recovery as a Service. Customer shall not be eligible to seek more than one (1) Service Credit per Out of Service

Condition for any given reason within a single calendar month. In the event an Out of Service Condition spans more than one (1) calendar month, the Out of Service Condition shall be defined as one (1) Out of Service Condition for the purpose of the Service Credit that Customer will be entitled to as outlined within this SLA.

14. **Termination Fees.** If the Customer terminates the Services for any reason other than for cause as permitted under the Agreement, or if Rogers terminates the Services for cause as permitted under the Agreement, Customer shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

i) fifty (50%) percent of the average monthly charges per terminated Service (as determined over the previous three (3) months, or if less than three months have passed, the average monthly charges for the Service Term per terminated Service) multiplied by the number of months remaining in the Initial Service Term or Renewal Service Term, as applicable, from the effective date of termination;
ii) all usage, taxes, and late payment charges incurred up to the date of termination; and
iii) one hundred percent (100%) of the non-recurring charges for the terminated Service(s).

Where Customer terminates the Services prior to the expiration of the Initial Service Term or Renewal Service Term, as applicable, Customer shall either return all Rogers Equipment associated with the Services to Rogers or pay to Rogers the fair market value of such Rogers Equipment.

The above shall be included in an invoice to Customer subsequent to termination.to Customer subsequent to termination.