

This document sets out provisions with respect to Data Centre and Cloud products and/or services provided by Rogers Communications Canada Inc. (“**Rogers**”) pursuant to a Rogers for Business Agreement (the “**Agreement**”). The applicable terms set forth below form an integral part the Agreement. Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Agreement.

By clicking on the links below, you will be redirected to the terms that are relevant for each named product and/or service.

[Colocation Services](#)

[Virtual Private Cloud Services](#)

[Veeam Cloud Connect](#)

[Disaster Recovery as a Service](#)

[Managed Private Cloud Services](#)

[Business Resumption](#)

[Managed Services](#)

[Managed Cloud Backup Services](#) (HFX)

[Object Store](#)

[Dedicated Backup Services](#)

[Cloud Backup Services](#)

[Managed Cloud Connect Services](#)

Colocation Services

The following terms pertain specifically to Colocation Services supplied by Rogers to you.

1. **Definitions.** Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:
 - 1.1 Acceptable Downtime means any of the following events: Scheduled Maintenance; Emergency Maintenance; your breach of the Agreement; order suspensions due to your credit worthiness; failure of your applications or your equipment not within the sole control of Rogers or its subcontractors; any act or omission by you or user of the Colocation Services authorized by you; any event of Force Majeure; power consumption that exceeds the power rating load or that does not maintain adequate balance across A and B Power Distribution Unit ("PDU") circuits (for the Power Availability Service Level Agreement only).
 - 1.2 Business Day means Monday to Friday inclusive, excluding statutory holidays observed in the Province of Ontario.
 - 1.3 Climate Control Availability means the percentage of time during a specific calendar month that the climate control (temperature and humidity) to the raised floor portion of the Colocated Site is within industry-acceptable parameters.
 - 1.4 Colocated Site means the physical Rogers data centre location in which your Space or equipment is made available by Rogers, as specified in the attached Agreement(s).
 - 1.5 Emergency Maintenance means any urgent maintenance activities performed on the Rogers' infrastructure connected to your Space or your equipment in order to prevent or address imminent failures affecting Rogers' infrastructure.
 - 1.6 End-user means any person enabled, through a data connection over the internet, to access, use, purchase, download, or otherwise interact with your content, which is located on or distributed by means of your equipment.
 - 1.7 High Availability Network Configuration means that you must utilize redundant network connections from their Colocation Services environment to the Rogers core Network.
 - 1.8 Monthly Recurring Charge – means the monthly charge for each Colocation Service.
 - 1.9 Network means Rogers owned and operated TCP/IP-based data communications network.
 - 1.10 Out of Service Condition means a condition whereby there is a Colocation Service outage, excluding any Colocation Service outage resulting from an Acceptable Downtime. For Redundant Power Configuration, failure of both A and B PDU circuit(s) at the same time will be considered an Out of Service Condition for Power Availability.
 - 1.11 Power Availability means the percentage of time during a specific calendar month that the power supply to a particular Space is available. Power Availability is based on ticket information from Rogers Customer Care. If an Out of Service Condition is detected or reported on a specific power supply, the power supply will be deemed to be unavailable for the length of the Out of Service Condition.
 - 1.12 Redundant Power Configuration means that you must utilize and consume power directly from both A and B PDU circuits.
 - 1.13 Scheduled Maintenance means any maintenance activities performed on the Rogers' infrastructure connected to your Space or your equipment provided that you shall be given at least five (5) Business Days in advance notice of such maintenance activities.
 - 1.14 Space means a designated section of the Colocated Site where space of one or more equipment cabinets (or racks) are set-aside by Rogers for your equipment.

- 1.15 Statement of Work means a document outlining the scope of a project to be completed by Rogers for you and describing the specifications and professional services required to execute the project.

2. Term, Rates, and Charges

- 2.1 The term of each Colocation Service (each an “**Initial Service Term**”) is as set forth in the Agreement(s). The term of this Schedule commences on the date of signature of the Agreement by you, or, if this Schedule is attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon expiration of the Initial Service Term, a Colocation Service may be renewed for an additional period set forth in the Agreement to be added to this Agreement by way of amendment (a “**Renewal Service Term**”) or, if no amendment is executed, the Colocation 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**”.
- 2.2 The Fees for the Colocation Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers’ equipment or Colocation Services by any third party or unauthorized person.
- 2.3 Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Monthly Recurring Charges set out in any applicable Agreement represent minimum charges. Such charges will commence as of the Service Effective Date. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 2.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Colocation Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Colocation Services 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 your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 2.5 You are responsible for all charges for excess usage beyond the minimum Monthly Recurring Charges billed at a twenty-five (25%) percent premium above the monthly rate. Unless otherwise specified, there are no limits or restrictions on usage.
- 2.6 Rogers reserves the right to change rates for any and all Colocation Services throughout the Service Term upon the provision of ninety (90) days’ written notice to you in the event of an increase in third party supplier costs.
- 2.7 Upon the commencement of a Month-to-Month Renewal Term for a Colocation Service, the rates for such Colocation Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 2.8 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

3. Your Equipment

- 3.1 You shall, at your own expense, supply, order, install, configure, engineer, troubleshoot, and maintain all of your equipment, including cabling and termination devices necessary to support network access. Unless otherwise stated in the Agreement, Rogers shall not provide any such services or provide any installation assistance. Upon completion of installation or maintenance on your equipment, you shall remove all of its installation tools and material from the Space and Colocated Site and shall restore the area around the Space to its pre-installation condition. Your failure to do so will constitute a material breach of the Agreement.
- 3.2 You shall remove all items of your equipment located in the Space within thirty (30) days of the date of termination of the Colocation Services. If your equipment has not been removed after thirty (30) days, Rogers shall charge you a premium storage rate calculated as 200% of the Monthly Recurring Charges for

Colocation Services. In the event that all or part of your equipment is still not removed within ninety (90) days of termination of the Colocation Services, it will be considered abandoned and Rogers may, without liability to you, remove your equipment and charge you for storage costs, plus any past due fees or charges.

- 3.3 In the event that you fail to pay amounts when due as set out in the Agreement, in addition to all remedies set out in the Agreement, Rogers may deny you access to the Space, remove your equipment from the Space, and secure your equipment and retain possession thereof as security for the payment of any amounts owed by you for Colocation Services under the Agreement.

4. Security Access and Fraud

- 4.1 You agree to implement and is solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Colocation Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Colocation Services, your equipment, including unmanaged Rogers' equipment, and your accounts.
- 4.2 Rogers shall limit physical access to the Space and use commercially reasonable efforts to prevent unauthorized access to your equipment and, as determined by Rogers, to identify security breaches. Where a situation is considered a security breach, Rogers shall notify you as soon as feasible and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 4.3 You are solely responsible for establishing access and user management controls that clearly identify individuals who have access to your Space, account administration, security, technical and/or billing rights ("**Access Control and User Management Controls**") and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to your Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential.
- 4.4 Rogers will track all access to your Colocation Services through an online ticketing system and ensure that those who requested access have all your necessary documented approvals prior to accessing your Colocation Services.
- 4.5 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Colocation Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.
- 4.6 In the event of any emergency that presents a risk of an Out of Service Condition, or damage to your equipment or data belonging to Rogers, a third party, the Colocated Site, or to any persons or property present therein, Rogers may rearrange your equipment as is reasonably necessary to respond to the emergency. Additionally, and only as necessary, Rogers may disconnect or remove your equipment if the emergency requires such disconnection or removal to avoid damage. Rogers shall use commercially reasonable efforts to notify you prior to rearranging, disconnecting or removing your equipment, and in any case will notify you thereafter.
- 4.7 Responsibility for End-users. Rogers shall have no obligations or liability whatsoever towards End-users in relation to the Colocation Services. You shall be solely responsible for providing your services, technical support, and any and all other services to End-users.

5. Site Access

- 5.1 You shall not seek to or acquire any rights or interest in the Space, the Rogers' Equipment or any portion of the Colocated Site as a result of the Agreement or its termination for any reason.

- 5.2 Rogers shall provide reasonable commercial physical access to the Space to your authorized individuals identified through your Access Control and User Management Controls (“**Authorized Individuals**”), subject to the terms and conditions of this Schedule, and may require that a Rogers authorized employee accompany Authorized Individuals. In such a case where you require that a Rogers authorized employee accompany Authorized Individual(s), then you shall give a minimum of four (4) hours advance notice to Rogers’ Corporate Support team (the technical support group at Rogers responsible for handling support requests from you for the Colocation Services) for access to any Colocated Site, unless otherwise indicated by Rogers, provided that in case of an emergency, such access may be delayed and Rogers shall provide a reasonable estimate of the duration of such delay. You shall be fully responsible for the acts and/or omissions of Authorized Individuals or agents inside the Colocated Site.
- 5.3 All visitors must present a valid government issued photo ID and be authorized in advance by you, subject to Rogers’ approval, to access your Space. If Rogers’ records indicate that a visitor is not designated as a Authorized Individual, the visitor will not be granted access to the Colocated Site.
- 5.4 All emergencies and suspicious behaviour noted at the Colocated Site by you must be immediately reported to the Rogers security desk.
- 5.5 Rogers reserves the right to inspect your Space upon the provision of reasonable advance notice and with you, or an Authorized Individual, present.

6. Insurance

- 6.1 You shall provide proof of insurance prior to installation of your equipment in the Space and maintain such insurance at all times during the Service Term for Colocation Services. Proof of insurance shall be provided by delivery of certificates of insurance to Rogers showing the following types of insurance, in the following minimum amounts, which insurance shall be issued by companies which have an A.M. Best’s Key Rating of at least A or higher:
- 6.1.1 Commercial general liability insurance including coverage for personal injury, bodily injury (including death), contractual liability, employer’s liability insurance, and broad form property damage, including loss of use of property, occurring in the course of or in any way related to your operations, with minimum limit of \$3 million per occurrence or such other reasonable amount that Rogers may require from time to time; and;
- 6.1.2 All risk property insurance covering your equipment located in the Space in an amount not less than its full replacement value. Such policy shall include a waiver of subrogation in favour of Rogers and its landlord.
- 6.2 Rogers and its landlord for each Colocated Site shall not insure or be responsible for any loss or damage to property of any kind owned or leased by you or your employees, servants, and agents, including but not limited to your equipment. The maintenance of insurance by you shall not affect or limit the extent of your liability under this Agreement.
- 6.3 Rogers shall be named as an additional insured on the Commercial general liability policy required above. During the Service Term for Colocation Services or any renewal thereafter, you or your Insurer shall provide 30 days’ prior written notice to Rogers of cancellation or material change adverse to Rogers of the policies described herein. Your Commercial general liability insurance policy shall be primary and non-contributing with any other insurance available to Rogers.

7. Optional Services

- 7.1 Professional Services. Professional services offered by Rogers to complete specific work requested by you are subject to additional charges and require your approval of a Statement of Work. Applicable charges include, but are not limited to travel, living, and miscellaneous expenses. You will also be responsible for all costs associated with the purchase, lease, and/or subscription of any software, hardware or related equipment required to fulfill the Statement of Work.

7.2 Data Centre Carrier Neutrality. Rogers may, in its sole discretion, allow third party network and access providers to provide connectivity to your Colocation Services, upon your request to Rogers and subject to additional charges. Rogers shall provision the cross-connection between your Space and the third party connectivity provider. You are 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.

7.3 Remote Hands. Rogers may make available personnel who will, upon your request and Rogers' personnel availability, provide non-technical support and assistance related to your equipment or Space ("**Remote Hands**"). Rogers shall quote a charge for such Remote Hands assistance to you, and upon your acceptance of such charges, response times will be based on commercially reasonable efforts. Remote Hands will act only upon request and direction from you. Rogers is not responsible or liable for any consequences of the actions performed upon your request by Remote Hands.

7.4 Relocation of your equipment. Relocation of your equipment to another part of the Colocated Site or another Colocated Site, may be requested by you. If approved by Rogers, it shall be performed by you or its subcontractors at your sole expense. Rogers is not responsible for any network access disruptions caused by relocation of your equipment.

7.5 Network Access. Where requested by you, and subject to additional charges, Rogers shall provide network access to the Space ("Network Access").

8. Product Service Level Agreement ("SLA")

8.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("**Service Credit**").

Table 1: Power Availability

	Power Availability	Service Level Credit
Redundant Power Configuration	100%	One (1) day of pro-rated monthly recurring charges for the impacted Colocation Services for each cumulative sixty (60) minutes or fraction thereof, up to 50% of the Monthly Recurring Charges for the impacted Colocation Services.
Non-Redundant Power Configuration	99.99%	One (1) day of pro-rated monthly recurring charges for the impacted Colocation Services for each cumulative sixty (60) minutes or fraction thereof, up to 50% of the Monthly Recurring Charges for the impacted Colocation Services.

Table 2: Climate Control Availability

Temperature	Humidity	Service Level Credit
Less than 59F / 15C for a period of 60 minutes or more	Less than 20% for a period of 60 minutes or more	One (1) day of pro-rated monthly recurring charges for the impacted Colocation Services for each cumulative sixty (60) minutes or fraction thereof, up to 50% of the Monthly Recurring Charges for the impacted Colocation Services.
More than 89.6F / 32C for a period of 60 minutes or more	More than 80% for a period of 60 minutes or more	One (1) day of pro-rated monthly recurring charges for the impacted Colocation Services for each cumulative sixty (60) minutes or fraction thereof, up to 50% of the Monthly Recurring Charges for the impacted Colocation Services.

Table 3: Network Availability*

	Network Availability	Service Level Credit
High Availability Network Configuration	100%	One (1) day of pro-rated monthly recurring charges for the impacted Colocation Services for each cumulative sixty (60) minutes or fraction thereof, up to 50% of the Monthly Recurring Charges for the impacted Colocation Services.

Non-High Availability Network Configuration	99.99%	One (1) day of pro-rated monthly recurring charges for the impacted Colocation Services for each cumulative sixty (60) minutes or fraction thereof, up to 50% of the Monthly Recurring Charges for the impacted Colocation Services.
---	--------	--

* If requested by you, and subject to additional charges

8.2 **Outage Notification.** You shall notify Rogers of any outage by opening a trouble ticket with Rogers Customer Care within one (1) day for any Power Availability or Climate Control Availability and ten (10) days for any Network Availability of any Out of Service condition, following which Rogers shall validate the outage. If Rogers determines that there is an outage, Rogers will record it as an Out-of-Service condition in its system.

8.3 **Monthly Service Level Credit Limitation.** The combined cumulative total of all Service Credits for a calendar month for the Colocation Services will not exceed the total Monthly Recurring Charges for the affected Colocation Sites that Rogers has invoiced for such calendar month.

8.4 **Service Credit Request Process.** If Rogers has failed to meet any of the above service levels for your particular Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.

8.5 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Colocation Services. You 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 you will be entitled to as outlined within this SLA.

9. **Termination Fees**

9.1 If you terminate the Colocation Services without cause, or if Rogers terminates the Colocation Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

- a) fifty (50%) percent of the average monthly charges per terminated Colocation 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;
- b) any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the applicable Colocation Service that exceeds the amount set out in (a) above; and
- c) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Colocation Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Colocation Service.

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

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

Virtual Private Cloud Services

The following terms pertain specifically to Virtual Private Cloud supplied by Rogers to you.

1. **Definitions.** Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:

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; your failure to comply with your obligations as defined in the Agreement, including failure to pay valid past-due amounts or any suspension of the Services due to your credit worthiness; failures of your applications or any of your 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; your acts or omissions or any use or user of the Virtual Private Cloud Services authorized by you; during an event of Force Majeure.

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;

Compute Availability - For you, 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 you to use made available to you from within vCloud Director.

Corporate Support Team - Corporate Support Team means the technical support group at Rogers' responsible for handling all support requests from you. The Corporate Support Team operates 24x7, x365. The support is provided from Canada, excluding any technical action which may be handled remotely from outside of Canada. Rogers Support is your primary point of contact for all information security requests by you. Support is available in English and French.

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 your Content. Where possible, and if the situation allows for it, you will be notified by Rogers within twenty-four (24) hours of any such Emergency Maintenance.

Host - The physical server on which the virtual machines reside.

Incident Management - An Incident means an unplanned interruption to any part of the Virtual Private Cloud Service or reduction in the quality of the Virtual Private Cloud Service. An Incident can be created by you 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.

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

Move/Add/Change/Delete (MACD) Request - MACD means your requests which are 'add-ons', changes or compliment the Virtual Private Cloud 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.

Network Availability - For you, Rogers will use its Platform Monitoring and Alarming system to poll the availability of each type of storage. Network means the External network on the WAN side of the NSX device made available to you from within vCloud Director.

Organization - Within the vCloud Director, you 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.

Out of Service Condition means a condition whereby there is Virtual Private Cloud Service outage, including lack of Virtual Private Cloud Service Availability.

Platform Monitoring and Alarming - The tools used by Rogers to determine the availability of the Virtual Private Cloud Service.

Response - measured from the time you call or create an Incident ticket in MyAccount Portal to the time a Rogers employee updates the ticket, speaks to, chats, or emails you.

Rogers Support System - The tools used by Rogers to record and track all Service Requests and Incidents Requests as part of the Virtual Private Cloud Service.

Scheduled Maintenance - Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected. You shall be given at least five (5) days advance notice of Scheduled maintenance activities. The details of the service window and your negative impact will be communicated to you in the notification.

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

Service Request - Service Request means a request from you 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 you 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.

Service Request Resolution - Service Request Resolution means that the Service Request has been completed and Rogers has communicated this to you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.

Site - Site means the physical location(s) in which your Virtual Private Cloud Services are made available by Rogers.

Standard / Performance Storage Availability - For you, Rogers will use its Platform Monitoring and Alarming system to poll the availability of each type of Storage. Storage means the Datastore made available to you from within vCloud Director.

Virtual Data Centre - Virtual Data Centre (VDC) is made up of the virtual compute, network and storage allocated to you as part of your Virtual Private Cloud Services.

Virtual Machine - The software representation of a computer system running on top of VMware vSphere.

2. **Features.** The Virtual Private Cloud Services (“**Services**”) include the following features:

Additional Managed Backup per virtual machine - These services are only available if you have contracted for Managed Services separate from these terms. This Additional Managed Backup per virtual machine consists of this one tier of services:

Fully Managed Backup - A service level where you have elected to have the Services backed up by Rogers for a monthly fee and a one-time setup cost.

Additional Managed Server per virtual machine - These services are only available if you have contracted for Managed Service separate from these terms. Three tiers of services are available as set out below:

Fully Managed services - A service level where you have elected to have the Services operated, maintained, monitored and patched by Rogers for a monthly fee and a one-time setup cost.

Proactive Monitoring/Patching/Reporting services - A service level where you have elected to have the virtual machines maintained, monitored, and patched by Rogers for a monthly fee and a one-time setup cost.

Self-Serve Monitoring and Alerting - A service level where you have elected to have the virtual machines monitoring enabled and transmitted to you by Rogers for a monthly fee and a one-time setup cost.

Compute Unit - A Compute Unit is a fixed ratio of vCPU to vRAM. The ratio for the Services is 1vCPU:2GB vRAM.

Dedicated Blade - Is a fixed physical server reserved for the exclusive use of only you. The capacity made available by Dedicated Blade(s) is express in Compute Units. The initial deployment of Dedicated Blades is a single pair, with an N+1 configuration, where one entire physical server is always reserved for failover and not available for Customer's non-emergency use. Additional Dedicated Blades can be added one at a time and will increase the number of available Compute Units.

Dedicated Storage - Your storage capacity is allotted increments of 1 Gigabyte (1 GB = 1,073,741,824 bytes). Storage is characterized in three ways as set out below. Selection of the storage device and its configuration can have an impact on the usable storage capacity. Rogers will provide the available Raw Storage (based on the physical attributes of the device) and the Effective Storage (based on industry standards and information provided by you) to you. Usable Storage is a result of many factors and will vary depending on your communicated requirements, selections, and overtime based on usage.

Effective Storage - how much storage is presented after advanced compression and deduplication is applied to the Raw Storage. The compression and de-duplication technologies can increase the available storage by

multiples and is expressed in the form of a ratio. 1:1 means no increase, 2:1 means double the Raw Storage, 3:1 means triple the Raw Storage and so on. This ratio is not guaranteed and varies depending on the types of content being written to the storage.

High Availability (HA) – Rogers maintains a sufficient number of physical resources to allow for virtual machines that reside on a failed server to restart on another server.

Hyperconverged Dedicated Blade – Is a fixed physical server reserved for the exclusive use of you. The capacity made available by Dedicated Blade(s) is expressed in Compute Units. The initial deployment of dedicated blades is a three-blade cluster, with an N+1 configuration. The equivalent compute resources to one physical host server are held in reserve for failover and are not available for Customer's non-urgent use. Additional Dedicated Blades can be added one at a time and will increase the number of available Compute Units which will also increase the amount of available storage. Storage is vSAN using physical hard drives (raw storage) dispersed through the dedicated blades. Storage is presented as Effective Storage.

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.

Linux based OS – Subscriptions of Centos Enterprise Linux (CEL) are available for a fee. CEL subscription are governed by the End User License Agreement described in section 11 below.

Microsoft based OS and Application Software – Subscriptions to a range of Microsoft Server OS and applications are available for a fee. All Microsoft subscriptions are governed by Microsoft Service Provider License Agreement (SPLA) and any End User License Agreement as described in section 11 below.

MyAccount Portal – The Rogers portal that you use to manage your user accounts, review billing information, open and review support tickets, purchase additional Services, and review your reporting.

Network – The Virtual Private Cloud contains virtualized network resources. Each Customer's Virtual Private Cloud has a VMware NSX logical device that controls and segregates your Content.

Organization – Through the MyAccount Portal, Customers can build logical Organizations in vCloud Director. These include users and policies, Virtual Datacentres, and catalogs (images and templates). Each Organization can be attached to one or more Virtual Datacentres.

Platform Management Monitoring and Alarming – the infrastructure supporting the Virtual Private Cloud Services is managed by Rogers. Management of the Virtual Private Cloud infrastructure, physical hosts, switching, storage, vCloud Director and ESXi includes; 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.

Professional Services - Where you request custom configuration of the Virtual Private Cloud Services beyond standard installation, Rogers will quote any required Professional Services to you in a separate Statement of Work.

Storage - Storage is connected to your VDC through the VMware vSphere. Storage in the Virtual Private Cloud comes in two types, Standard and Performance.

Raw Storage - the physical storage provided without the use of any compression or de-duplication. Raw Storage is calculated by adding up the capacity of all the physical storage in the device.

Usable Storage: This represents the amount of storage available for you to store your content. To calculate the Usable Storage, subtract all overhead for the management from the Effective Storage. VSAN automatically consumes additional storage to protect data stored within its datastores based on the data protection configuration of the cluster.

Virtual Data Centre (VDC) – A VDC is made up of a resource pool or collection of virtual CPU, RAM, network and storage resources allocated to you. The virtual representation of these resources is called vCPU, vRAM, vNetworks, and Datastores.

VMware vCloud Director – The VMware portal that presents the Services to you to self-administer. The vCloud Director is the primary tool that you will use to access the Services and maintain user permissions.

VMware vSphere – The virtualized environment on which your Services run is VMware ESXi.

3. Term, Rates, and Charges

- 3.1 The term of this Schedule commences on the date of signature of the Agreement by you, or inclusion of this Schedule to the Agreement by way of amendment and ends on the expiration of the last in force Service Term. The term of each Virtual Private Cloud Service (each an “**Initial Service Term**”) is as set forth in the Agreement(s). Upon expiration of the Initial Service Term, a Virtual Private Cloud Service may be renewed for the additional period set forth in the Agreement to be added to this Agreement by way of amendment (a “**Renewal Service Term**”) or, if no amendment is executed, the Virtual Private Cloud 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**”.

- 3.2 The Fees for the Virtual Private Cloud Services, including the Monthly Recurring Charges are set out in the Agreement(s). Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers’ equipment or Virtual Private Cloud Services by any third party or unauthorized person.
- 3.3 Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Such charges will commence as of the Service Effective Date. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 3.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Virtual Private Cloud Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Virtual Private Cloud Services or thirty (30) days after the Service is made available to you by Rogers in accordance with this Schedule. In the first month, the charges will be prorated for the number of days in the month after the Service Effective Date. Rogers will, by way of invoice or otherwise, notify you of the Service Effective Date. Applicable Service Credits will be applied to your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 3.5 Monthly Recurring Charges set out in any applicable Agreement represent minimum charges. you are responsible for all charges for excess usage beyond the minimum Monthly Recurring Charges billed at a twenty-five (25%) percent premium above the monthly rate. Unless otherwise specified, there are no limits or restrictions on usage. If you purchase 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.
- 3.6 Rogers reserves the right to change rates for any and all Virtual Private Cloud Services throughout the Service Term upon the provision of ninety (90) days’ written notice to you in the event of an increase in third party supplier costs.
- 3.7 Upon the commencement of a Month-to-Month Renewal Term for a Virtual Private Cloud Service, the rates for such Virtual Private Cloud Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 3.8 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

4 **User Subscription types (Standard and Principal)**

Access to the Services is configured for two (2) types of users as set out below. Your account will specify the user type. The two available user types are:

- a) **Standard User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below.
 - Use of the Virtual Private Cloud resources.
- b) **Principal User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below:
 - Purchasing additional Services through the “Buy More” function;
 - Adding Standard Users to the Services;
 - Responsible for keeping the account information up to date;
 - Responsible for providing your current contact information for Rogers automatic notification systems;
 - Responsible for receiving all notices from Rogers relating to the Services.

5 **Your Responsibilities** and acceptable use policy:

- 5.1 You bear all risk associated with your use of the Services.
- 5.2 You are responsible to ensure that the Services are sufficient for your needs.

- 5.3 You are solely responsible to determine that your use of the Services is compliant with all laws and regulations applicable to you.
- 5.4 You agree to use the Services in compliance with all applicable laws and regulations, including, without limitation applicable privacy laws.
- 5.5 You agree not to use the Services:
 - 5.5.1 To violate or infringe on the rights of other customers;
 - 5.5.2 To use the Services to gain unauthorized access to or to disrupt in any manner any third-party service, device, data account or network;
 - 5.5.3 To spam or distribute malware;
 - 5.5.4 In any way that could harm the Services or impair other's users use of the Services;
 - 5.5.5 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.
- 5.6 To the extent required by applicable laws and your own business requirements, you shall retain connection logs, or any data required to identify any internal or other user of your own services hosted on the Services.
- 5.7 You 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.
- 5.8 You are solely responsible for use of the Services by any individual to whom you may have provided your password(s) and any other means of access (such as SSH access keys, API, etc.).
- 5.9 You are solely liable for the consequences of the loss of any passwords and any other means of access to the Services.
- 5.10 You are responsible for providing appropriate staff to participate in troubleshooting incidents and service requests. During an incident or a service request you will actively participate in the resolution of the request. Any time spent waiting for communications from you may result in the severity of the ticket getting downgraded and the time subtracted from the resolution time.
- 5.11 You are responsible for coordinating all communications with any third party you have contracted to provide any type of support for your services.
- 5.12 You are responsible for maintaining strong password to access the Services. Changes to the access controls require the provision of your designated secure username and password. Credentials designated by you must utilize strong security traits (e.g., upper and lower case values, numeric and non-numeric values). You are responsible for credentials and must keep credentials secure and confidential.
- 5.13 You shall be solely responsible for providing your services, technical support, pricing and service plans, billing and collections, and any and all other services to your end users, and Rogers shall have no obligations or liability whatsoever to end users in relation to the Virtual Private Cloud Services.
- 5.14 You 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. You agree to pay any such charges based on use of the Services by your end users.
- 5.15 You agree that it may be required to participate in a Rogers compliance audit with regard to any of your obligations relating to the Services, including but not limited to the obligations set out in these terms.
- 5.16 Violation of the terms in this section may result in suspension of the Services. Rogers may, at its sole discretion suspend the Services only to the extent reasonably necessary.
- 5.17 Unless Rogers believes an immediate suspension of your Services is required, Rogers will use reasonable efforts to provide notice before suspending your Services.
- 5.18 The Services will continue on a month-to-month basis after the end of the Service Term with the following conditions:
 - 5.18.1 You are responsible for making arrangements for the renewal or termination of the Services.
 - 5.18.2 Failing such arrangements, Rogers may, in its sole discretion, terminate the Services upon thirty (30) days' written notice.
- 5.19 Upon the termination or expiration of the Services, Rogers will contact you in writing through the Principal User informing you that your Content must be removed from the VDC (the "**Content Removal Notice**"). You will have thirty (30) days from the date of the Content Removal Notice to make arrangements to remove your Content from the VDC. Any assistance provided to you by Rogers related to your Content may be billable to you at Rogers' then current time and materials rates. Thirty (30) days after providing the Content Removal Notice to you, Rogers has the right to remove any of your remaining Content from the VDC in any manner, including deletion.

6 Your Indemnity

In addition to the indemnification provisions set out in the Agreement, you 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 you agrees to lawfully obtain any licences required, if any, to use any third-party intellectual property, including software; (ii) for the use of any third-party licenses including but not limited to, Microsoft, Red Hat, and Oracle, ; (iii) and for any third-party content.

7 Backup, Content Integrity and Disaster Recover

- 7.1 **Backup Services.** Rogers is not responsible for providing, or for any cost or expenses associated with providing, any administrative, technical, emergency or support personnel associated with the Virtual Private Cloud Services or for providing and maintaining your Content (defined below) on the Virtual Data Centre.
- 7.2 Notwithstanding anything to the contrary, the Services do not backup your Content as part of the Services. You agree to take all the necessary measures to back up your Content in the event of data loss/Content loss or deterioration of your Content, whatever the cause.
- 7.3 For greater certainty, the inclusion of data replication (as part of resiliency) shall not be considered “data backup” for the purposes hereof.
- 7.4 You are solely responsible to set up your own business continuity plan and/or business recovery plan.

8 Services and Networking.

- 8.1 **Compute Access:** If you are managing your own Virtual Private Cloud Services, you will be permitted to turn up and take down virtual machines as required. This includes virtual network devices.
- 8.2 **Network Access:** The Services include access to a shared internet connection with a maximum throughput of 250Mbps. You will access the Services by way of this shared internet connection. If you require private or dedicated network access, you can purchase a Rogers Wireline service for a fee.
- 8.3 **Data Centre Carrier Neutrality:** Rogers will, in its sole discretion, allow third party network and access providers to provide connectivity to your Virtual Private Cloud Services. Rogers will provision the cross-connection between your Virtual Private Cloud space and the third party connectivity provider. You are 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 Virtual Data Centre:** You will under no circumstances be permitted to access the physical space or the surrounding facility from which the Virtual Private Cloud Services are performed. You will not acquire any interest in, nor file any liens upon, the Virtual Data Centre, the Rogers Equipment, and any portion of the data centre as a result of the provision by Rogers of the Virtual Private Cloud Services 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 you. Rogers will ensure that you do not disrupt the use of other users of the Services. Rogers will prevent Noisy Neighbours and will generally limit your ability to adversely affect other users and other Customers. Noisy Neighbor means you 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 you are a Noisy Neighbour Rogers may, and Rogers reserves the right to temporarily limit your use of the Services. Rogers will attempt to contact you prior to any corrective action. Any action by Rogers to address a Noisy Neighbour and any disruption to your Services is excluded from the SLA for the Services.
- 8.6 **Measures for the prevention of spamming:** You are 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.

8.7 Remote Site Internet: You will access the Services remotely via the internet. You must have your own local internet connection to access the Services, and is solely responsible for the aforementioned internet connection, in particular its availability, reliability and security.

9 Security Access and Fraud.

- 9.1 You agree to implement and are solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Virtual Private Cloud Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Virtual Private Cloud Services, your equipment, including unmanaged Rogers equipment, and your accounts.
- 9.2 Rogers shall limit physical access to the Virtual Private Cloud Services and use commercially reasonable efforts to prevent unauthorized access to the Virtual Data Centre and, as determined by Rogers, to identify security breaches. Where a situation is considered a security breach, Rogers shall notify you as soon as feasible and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 9.3 You are solely responsible for establishing access and user management controls that clearly identify individuals who have access to your Space, account administration, security, technical and/or billing rights ("**Access Control and User Management Controls**") and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to your Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential.
- 9.4 Rogers will track all access to your Virtual Private Cloud Services through an online ticketing system and ensure that those who requested access have all your necessary documented approvals prior to accessing your Virtual Private Cloud Services.
- 9.5 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Virtual Private Cloud Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.
- 9.6 In the event of any emergency that presents a risk of an Out of Service Condition, or damage to your equipment or data belonging to Rogers, a third party, the Colocated Site, or to any persons or property present therein, Rogers may rearrange your equipment as is reasonably necessary to respond to the emergency. Additionally, and only as necessary, Rogers may disconnect or remove your equipment if the emergency requires such disconnection or removal to avoid damage. Rogers shall use commercially reasonable efforts to notify you prior to rearranging, disconnecting or removing your equipment, and in any case will notify you thereafter.
- 9.7 You are solely responsible for user access security or network access security with respect to your Content.
- 9.8 All Content within the Virtual Data Centre is completely isolated through the use of industry standard virtualization protocols and VLAN rules within the infrastructure. You are further isolated with virtual firewalls. All Content will be located within the Virtual Data Centre which is housed within one of Rogers' data centre facilities located within Canada.
- 9.9 You are not permitted to run security penetration tests on the Virtual Private Cloud Services 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 you perform invasive platform testing without written approval.

- 9.10 To maintain the level of security for your Services, Rogers may update the operating systems before pre-installing them on the Services. You acknowledge that ensuring the level of security may cause an impact on your use of the Services. Notwithstanding the foregoing, Rogers shall use commercially reasonable efforts to avoid material impact on the functionality of the Services, subject to patches of third party products, which Rogers does not control.
- 9.11 To the extent practicable, updates are performed in collaboration with you. For any avoidance of doubt, after the delivery of the Service to you, the responsibility to manage and update of the operating systems and pre-installed applications is transferred to you.
- 9.12 Notwithstanding the foregoing, Rogers reserves the right to request that you install updates and patches in connection to running Services. If you fail 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 your Content or the Services or to Rogers, its Subcontractors, or other customers, Rogers may suspend access to the Service(s) until you comply with such request, or the Service is reinstalled.
- 9.13 If Rogers detects or reasonably believes that your usage represents a security risk, an email will be sent to you, 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.
- 9.14 In case of a security breach Rogers reserves the right to suspend the Services immediately in order to maintain the integrity of your Content.
- 9.15 Manipulations consisting of transferring data/Content from the affected system to the new system must be done by you. Rogers will provide reasonable assistance to you to create a new system using the Services provided under these terms. Professional Services can be purchased by you to perform work outside of the Services set out in these terms. Rogers is under no obligation to meet your needs in this regard and any professional services are provided at Rogers sole discretion.
- 9.16 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 your data/Content, or (b) your 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. You acknowledge that such suspensions do not release it of any obligation to pay for the Services.
- 9.17 Rogers shall not be held responsible for your usage of the VMware vCloud Director API, notably for any misuse of the Services by you through the API.

10 **Support**

- 10.1 When reporting an incident and creating a ticket for the purposes of technical support, you agree to provide Rogers with all relevant information reasonably required for the diagnosis and intervention of the incident.
- 10.2 You undertake 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 you to provide Rogers access to your Service. If you are 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**

- 11.1 Upon purchase of Virtual Private Cloud Services by you, Rogers will grant to you a license for Virtual Data Centre operating systems (OS) and associated Software. These licenses are subject to and subordinate to the underlying End User License Agreement (EULA) from the OS or Software licensor.
- 11.2 You agree you have read and understood the following EULAs if making use of any such services:

- 11.2.1 EULA for Microsoft OS licenses is located here:
[https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms\(WW\)\(ENG\)\(Apr2014\)\(CR\).pdf](https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms(WW)(ENG)(Apr2014)(CR).pdf)
- 11.2.2 EULA for VMWare is located here:
https://myaccount.datacentres.rogers.com/legal/vmware_universal_eula.pdf
- 11.2.3 EULA for Redhat is located here:
https://myaccount.datacentres.rogers.com/legal/GLOBAL_EULA_RHEL_English_20101110.pdf

- 11.3 Any licenses provided by Rogers to you for your Virtual Private Cloud Services are solely permitted for use upon the Virtual Data Centre infrastructure. Upon termination of the Virtual Private Cloud Services for any reason, these licenses shall be terminated, and you shall have no further rights to the Software, except as necessary to comply with the Agreement. For greater clarity, “you” in the above paragraph shall also include all end users.
- 11.4 You will have the right to provide your own OS and associated software licensing to be used on the Virtual Data Centre platform. You agree that, in the event you provide your own OS and associated software licenses, you have taken all necessary steps to ensure that the licenses being used are legally licensed and supported through an agreement between you and the software provider. You will, if required by Rogers, provide proof of purchase for all Customer-provided licensing being used on the Virtual Data Centre platform.
- 11.5 If you makes use any non-Rogers provided software, you represent and warrant to Rogers that you have the right and applicable license to use the software in that manner.
- 11.6 If Rogers has agreed to provide management services, then you represent and warrant that your software license agreement with the software provider permits Rogers to perform these activities.
- 11.7 You are responsible for reporting to Rogers any changes to your use of the Services including but not limited to the virtual private cloud, virtual machines, or software agreements that impact your compliance with any software EULA. If you fail to disclose such changes you are liable for any incremental software licensing fees incurred by Rogers from the time of the change

12 **Content**

- 12.1 Definition of your Content. Your Content is defined as any software (including machine images), data, text, audio, and video or images that you or any user transfers to Rogers for processing, storage or hosting by the Services in connection with your account and any computational results that you or any user derives from the foregoing through your use of the Services.
- 12.2 Your Content does not include account information. The terms of the Agreement or other agreement with us governing the use of Services apply to your Content.
- 12.3 Ownership of Content. All interest in and ownership of Content including, but not limited to, those portions of the Content that are your trade names, trademarks or service marks, are and shall remain your property.
- 12.4 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 your Content located in the Virtual Private Cloud.
- 12.5 You shall remove all Content from the Virtual Data Centre prior to the date of termination of the Virtual Private Cloud Services. In the event that the Content is not removed, such Content will be considered abandoned, and Rogers may, without liability to you, delete the Content.
- 12.6 When evaluating the security of a cloud solution, it is important for you to understand and distinguish between the following:
 - 12.6.1 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.

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

12.7 If you have contracted for managed services with Rogers please refer to such other terms.

13 Product Service Level Agreement (“SLA”) and Service Level Objective (“SLO”)

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

Table 1: Power Availability

	Power Availability	Objective	Service Level Credit
Compute Availability	Less than 99.99%	Virtual Machine (VM): Poll the organization in vCloud Director at each Site and each Organization every five (5) min. for every VM and record a value of UP or DOWN. Host: Poll the Organization in vCloud Director every five (5) min. for every Host and record a value of UP or DOWN. If Host AND Virtual Machine are both DOWN perform the following calculation: Impact = SUM(VM_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 you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.
Network Availability	Less than 99.99%	Poll at each Site and Organization in vCloud Director NSX every 5 min. for connectivity to the Internet or Wide Area Network (WAN) and record a value of UP or DOWN. 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 you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.
Standard Storage Availability	Less than 99.99%	Poll at each Site and Organization in vCloud Director every five (5) min. for connectivity to the Standard Storage hardware and record a value of UP or DOWN. 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 you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.
Performance Storage Availability	Less than 99.99%	Poll at each Site and Organization in vCloud Director every five (5) min. for connectivity to the Performance Storage hardware and record a value of UP or DOWN. 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 you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.

VMware vCloud Director (vCD API services and vCloud Director Web Portal including access to your VM's, deploying new VM's, managing VM's)	Less than 99.99%	Poll each Site and Organization every 5 min. for connectivity to the vCloud Director and record a value of UP or DOWN. 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 you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.
MyAccount Portal (MyAccount API and MyAccount Web Portal)	Less than 99.99%	Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN. Impact = 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 you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you 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 you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Six (6) Hours	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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 you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Fourteen (14) Hours	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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 you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Seventy-two (72) Hours	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.
Service Request	Response Time Target as indicated below.	Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours Service Request Resolution Target: Five (5) Business Days (Monday to Friday 8am to 8pm EST)	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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 you call in live 24x7 = Live answer When you create in MyAccount Portal =	SLO Only (no service credit)

		Two (2) hours	
		MACD Request Resolution Target: Scoping performed on a case by case basis	

13.2 Incident Management Severity Levels:

- 13.2.1 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 your Content is at a significant risk of loss or corruption; You have had a substantial loss of service; and your business operations have been severely disrupted.
- 13.2.2 Severity 2: Major functionality is severely impaired. High impact; and Degradation of critical service or total of loss non-critical services
- 13.2.3 Severity Level 3 (S3) Partial, non-critical loss of functionality of the Services. Low impact – no direct business impact; and Non-critical services affected;
- 13.2.4 Service Request: A request from you 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).
- 13.2.5 Move/Add/Change/Delete (MACD) Request: Are requests which are 'add-ons' or compliment the Object Store 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.

13.3 Calculation for Response Time and Resolution Target for Incident Management (except if SLO):

- 13.3.1 Response Time Target Rogers response time will be measured from the time you call or create 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 you.
- 13.3.2 Rogers' resolution will be measured from the time you call or create an Incident ticket in MyAccount Portal (Rogers Support System) to the time a Rogers employee updates the Rogers Support System ticket informing you the incident is resolved.

13.4 Monthly Service Level Credit Limitation. 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.

13.5 Service Credit Request Process. If Rogers has failed to meet any of the above service levels for a particular Site of yours in any given billing month, you 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 you.

13.6 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Object Store Services. You 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 you will be entitled to as outlined within this SLA.

14 Termination Fees

14.1 Except as otherwise stated in Section 14.3 below, if you terminate the Virtual Private Cloud Services without cause, or if Rogers terminates the Virtual Private Cloud Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

- (a) Fifty percent (50%) of the monthly recurring charges for the terminated Service(s) multiplied by the number of months remaining in the Service Term from the effective date of termination; and
- (b) One hundred percent (100%) of the non-recurring charges for the terminated Service(s).

- 14.2 Where you terminate the Virtual Private Cloud Services prior to the expiration of the Initial Service Term or Renewal Service Term, as applicable, you shall either return all Rogers Equipment associated with the Virtual Private Cloud Services to Rogers or pay to Rogers the fair market value of such Rogers Equipment.

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

- 14.3 Trial Period. For the first sixty (60) days of the Initial Service Term, Rogers will offer you the Virtual Private Cloud Services ("**Trial Services**") on a trial basis (the "**Trial Period**"). Prior to the conclusion of the Trial Period, you must notify Rogers in writing if you wish to terminate the Trial Services. Failing such written notification prior to the conclusion of the Trial Period, you agree to purchase the Virtual Private Cloud Services described herein for the duration of the Initial Service Term at the rates set out in the Agreement.

Veeam Cloud Connect

The following terms pertain specifically to Veeam Cloud Connect Services supplied by Rogers to you.

1. Definitions. Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:

- 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; your failure to comply with your obligations as defined in the Agreement, including failure to pay valid past-due amounts or any suspension of the Services due to your credit worthiness; failures of your applications or any of your equipment not within the sole control of Rogers or a party under contract with Rogers to provide services in connection with the Agreement; acts or omissions of you or any use or user of the Veeam Cloud Connect Services authorized by you; 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 you. 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 Emergency Maintenance – Emergency Maintenance means any maintenance activities performed to prevent potential failures to infrastructure on which your services are connected or avoid a security breach that could compromise Your Content. Where possible, and the situation allows for it, you will be notified by Rogers within twenty-four (24) hours of any such Emergency Maintenance.
- 1.5 Incident Management – An Incident means an unplanned interruption to any part of the Veeam Cloud Connect Service or reduction in the quality of the Veeam Cloud Connect Service. An Incident can be created by you by 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.
- 1.6 Incident Management Resolution – Incident Management Resolution means that the service has been restored as per the SLA and this resolution has communicated to you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.
- 1.7 Infrastructure Refresh – All equipment manufacturer guarantees, warranties and service agreements are purchased by Rogers and maintained by Rogers. Rogers will refresh hardware as needed to support the Services.
- 1.8 Move/Add/Change/Delete (MACD) Request – MACD means your requests which are 'add-ons', changes or compliment the Veeam Cloud Connect 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.
- 1.9 MyAccount Portal – The Rogers portal that you use to manage your user accounts, review billing information, open and review support tickets, purchase additional Services, and review your reporting.
- 1.10 Out of Service Condition means a condition whereby there is a Veeam Cloud Connect Service outage, including any lack of Veeam Cloud Connect Services Availability.

- 1.11 Platform Management Monitoring and Alarming – the infrastructure supporting the Veeam Cloud Connect Services is managed by Rogers. Management of the Veeam Cloud Connect infrastructure, physical hosts, switching, storage, includes 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.
- 1.12 Platform Monitoring and Alarming – The tools used by Rogers to determine the availability of the Veeam Cloud Connect Service.
- 1.13 Professional Services - Where you request custom configuration of the Veeam Cloud Connect Services beyond standard installation, Rogers will quote any required Professional Services to you in a separate Statement of Work.
- 1.14 Response - measured from the time you call or create an Incident ticket in MyAccount Portal to the time a Rogers employee updates the ticket, speaks to, chats, or emails you.
- 1.15 Rogers Support System - The tools used by Rogers to record and track all Service Requests and Incidents Requests as part of the Veeam Cloud Connect service.
- 1.16 Scheduled Maintenance - Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected. You shall be given at least five (5) days advance notice of Scheduled maintenance activities. The details of the service window and your negative impact will be communicated to you in the notification.
- 1.17 Self-Service – Self Service means any operation carried out by you using an available tool provided by Rogers without submitting a ticket or contacting the Corporate Support Team.
- 1.18 Service(s) – Rogers' Veeam Cloud Connect Service(s).
- 1.19 Service Request – Service Request means a request from you 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 you 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.
- 1.20 Service Request Resolution – Service Request Resolution means that the Service Request has been completed and Rogers has communicated this to you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.
- 1.21 Site - This means the physical location(s) in which your Veeam Cloud Connect Services are made available by Rogers.
- 1.22 Veeam Cloud Connect Availability - For you, Rogers will use its Platform Monitoring and Alarming system to poll the availability of the Veeam Cloud Gateway to the external network and the underlying storage.
- 1.23 Veeam Cloud Connect Storage – The pooled storage resources (in GB) that stores all virtual machine, workstation, and physical service data in the Veeam Cloud Connect service offered by Rogers.
- 1.24 Veeam Cloud Connect Physical Server – The license to back up a single physical server to the Veeam Cloud Connect service offered by Rogers.
- 1.25 Veeam Cloud Connect Virtual Machine – The license to back up a single Virtual Machine to the Veeam Cloud Connect service offered by Rogers.
- 1.26 Veeam Cloud Connect Workstation – The license to back up a single Workstation (compute with a non-server-based operating system) to the Veeam Cloud Connect service offered by Rogers.

2. Term, Rates, and Charges

- 2.1 The term of each Veeam Cloud Connect Service (each an “**Initial Service Term**”) is as set forth in the Agreement(s). These terms commence on the date of signature of the Agreement by you, or, if these terms are attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon expiration of the Initial Service Term, Veeam Cloud Connect Services may be renewed for an additional period set forth in a Agreement to be added to this Agreement by way of amendment (a “**Renewal Service Term**”) or, if no amendment is executed, the Services 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**”.
- 2.2 The Fees for the Veeam Cloud Connect Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Professional Service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers’ equipment or Veeam Cloud Connect Services by any third party or unauthorized person.
- 2.3 Monthly Recurring Charges are set out in any applicable Agreement, representing minimum charges and are invoiced monthly, in advance, on the first day of each month. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 2.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Veeam Cloud Connect Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Veeam Cloud Connect Services or thirty (30) days after the Service Effective Date in accordance with these terms. 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 start date. Applicable Service Credits will be applied to your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 2.5 Consumption of Rogers Veeam Cloud Connect Services is metered using a “High Water Mark”. This is the peak total amount of the service used in a Calendar Month. Once the peak is achieved, it remains at that level until the end of the Calendar Month when it is reset. The charges set out in the Agreement represent the “High Water Mark” GB rate for the committed rate term. You will be responsible for all usage charges incurred. Unless otherwise specified, there are no limits or restrictions on usage.
- 2.6 If you purchase 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.
- 2.7 Rogers reserves the right to change rates for any and all Veeam Cloud Connect Services throughout the Service Term upon the provision of ninety (90) days’ written notice to you in the event of an increase in third party supplier costs.
- 2.8 Upon the commencement of a Month-to-Month Renewal Term for Veeam Cloud Connect Services, the rates for such Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 2.9 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

3. User Subscription types (Standard and Principle)

- 3.1 Access to the Services is configured for two (2) types of users as set out below. Your account will specify your user type. The two available user types are:
- c) **Standard User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below:
- Use of the Veeam Cloud Connect resources.

- d) **Principle User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below:
- Purchasing additional services through the “Buy More” function;
 - Adding Standard Users to the Services;
 - Responsible for keeping the account information up to date;
 - Responsible for providing your current contact information for Rogers automatic notification systems;
 - Responsible for receiving all notices from Rogers relating to the Services.

4 Your Responsibilities and Acceptable Use Policy:

- 4.1 You must have Veeam Backup & Replication software (purchased separately) to use the Rogers Veeam Cloud Connect Service.
- 4.2 You must license all Veeam Backup & Replication software correctly with the software providers' requirements.
- 4.3 You must ensure that the version of Veeam Backup & Replication used is compatible with the version of Veeam Cloud Connect offered by Rogers. Rogers will publish the version of Veeam Cloud Connect and notify you of 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, technical, emergency or support personnel associated with the restoration of the Veeam Cloud Connect Services due to you performing any changes to your own Veeam Backup & Replication software.
- 4.4 You bear all risk associated with your use of the Services.
- 4.5 You are responsible to ensure that the Services are sufficient for your needs.
- 4.6 You are solely responsible to determine that your use of the Services is compliant with all laws and regulations applicable to you.
- 4.7 You agree to use the Services in compliance with all applicable laws and regulations, including, without limitation applicable privacy laws.
- 4.8 You agree not to use the Services:
 - 4.8.1 To violate or infringe on the rights of other customers;
 - 4.8.2 To use the Services to gain unauthorized access to or to disrupt in any manner any third party service, device, data account or network;
 - 4.8.3 To spam or distribute malware;
 - 4.8.4 In any way that could harm the Services or impair other's users use of the Services;
 - 4.8.5 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.
- 4.9 To the extent required by applicable laws and your own business requirements, you shall retain connection logs, or any data required to identify any internal or other user of your own services hosted on the Services.
- 4.10 You are solely responsible for use of the Services by any individual to whom you may have provided your password(s) and any other means of access (such as SSH access keys, API, etc.).
- 4.11 You are solely liable for the consequences of the loss of any passwords and any other means of access to the Services.
- 4.12 You are responsible for providing appropriate staff to participate in troubleshooting incidents and service requests. During an incident or a service request you will actively participate in the resolution of the request. Any time spent waiting for communications from you may result in the severity of the ticket getting downgraded and the time subtracted from the resolution time.
- 4.13 You are responsible for coordinating all communications with any third party you have contracted to provide any type of support for your services.
- 4.14 You are responsible for maintaining strong password to access the Services. Changes to the access controls require the provision of your designated secure username and password. Credentials designated

by you must utilize strong security traits (e.g., upper and lower case values, numeric and non-numeric values). You are responsible for credentials and must keep credentials secure and confidential.

- 4.15 You shall be solely responsible for providing your services, technical support, pricing and service plans, billing and collections, and any and all other services to your end users, and Rogers shall have no obligations or liability whatsoever to end users in relation to the Veeam Cloud Connect Services.
- 4.16 You 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. You agree to pay any such charges based on use of the Services by your end users.
- 4.17 In addition to the indemnification provisions set out in the Agreement you 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 you agree 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.
- 4.18 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.
- 4.19 Unless Rogers believes an immediate suspension of your Services is required, Rogers will use reasonable efforts to provide notice before suspending your Services.
- 4.20 The Services will continue on a month-to-month basis after the end of the Term with the following conditions:
 - 4.20.1 You are responsible for making end of the Term arrangements by renewing your Services or cancelling the Services.
 - 4.20.2 If you do not make end of Term arrangements then Rogers may, in its sole discretion, terminate the Services.

5 Your Indemnity

In addition to the indemnification provisions set out in the Agreement, you 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 you agree 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; and (iii) any third-party content.

6 Backup, Content Integrity and Disaster Recover

- 6.1 Backup Restoral Services. Rogers is not responsible for providing, or for any cost or expenses associated with providing, any administrative, technical, emergency or support personnel associated with the restoration of your Content from Veeam Cloud Connect Services through the Veeam Backup & Replication software.
- 6.2 You agree to take all the necessary measures to back up your Content in the event of data loss or deterioration of your Content, whatever the cause.
- 6.3 You are solely responsible to set up your own business continuity plan and/or business recovery plan.

7 Services and Networking

- 7.1 Veeam Backup & Replication: You will manage your Content in the Rogers Veeam Cloud Connect Service through the use of your acquired and managed Veeam Backup & Replication software.
- 7.2 Network Access: The Services include access to a shared internet connection with a maximum throughput of 250Mbps. You will access the Services by way of this shared internet connection. If you require private or dedicated network access, you can purchase a Rogers Wireline service.

- 7.3 Ownership of Data Centre: You will under no circumstances be permitted to access the physical space or the surrounding facility from which the Veeam Cloud Connect Services are performed. You 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 Veeam Cloud Connect Services or your termination for any reason pursuant to the Agreement.
- 7.4 Fair Use of the Services: The Services are subject to fair use by you. Rogers will ensure that You do not disrupt the use of other users of the Services. Rogers will prevent Noisy Neighbours and will generally limit the ability of you to adversely affect other users and other customers. Noisy Neighbor means you 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 you are a Noisy Neighbour Rogers may, and Rogers reserves the right to temporarily limit your use of the Services. Rogers will attempt to contact you prior to any corrective action. Any action by Rogers to address a Noisy Neighbour and any disruption to your Services is excluded from the SLA for the Services.
- 7.5 Client-Side Internet: You will access the Services remotely via the internet. You must have your own local internet connection to access the Service, and are solely responsible for the aforementioned internet connection, in particular its availability, reliability and security.

8 Security Access and Fraud

- 8.1 You agree to implement and is solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Veeam Cloud Connect Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Veeam Cloud Connect Services, your equipment, including unmanaged Rogers equipment, and your accounts. You are solely responsible for user access security or network access security with respect to your Content.
- 8.2 Rogers shall use commercially reasonable efforts to prevent unauthorized access to Veeam Cloud Connect Services. Where a situation is considered a security breach, Rogers shall notify you as soon as commercially reasonable and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 8.3 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, Services and/or your data, or (b) your breach of the Agreement. In case of a security breach Rogers reserves the right to suspend the Services immediately in order to maintain the integrity of your content. 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. You acknowledge that such suspensions do not release it of any obligation to pay for Services.
- 8.4 You are solely responsible for user access security or network access security with respect to your Content and for establishing access and user management controls that clearly identify individuals who have access to account administration, security, technical and/or billing rights ("**Access Control and User Management Controls**") and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to your Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential. You are responsible for any use of the account regardless of who uses the Services.
- 8.5 Rogers will track all access to your Services through an online ticketing system and ensure that those who requested access have all your necessary documented approvals prior to accessing your Veeam Cloud Connect Services.

- 8.6 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you. If Rogers cannot verify your identity or suspects that there may be fraudulent or illegal activity Rogers may decline the request. In such an instance Rogers will attempt to contact the main or alternative contact.
- 8.7 In the event of any emergency that presents a risk of an Out of Service Condition, or damage to Rogers equipment or data belonging to Rogers, a third party, the Site or Rogers' data centre facilities, or to any persons or property present therein, Rogers may disable Veeam Cloud Connect Services as is reasonably necessary to respond to the emergency.
- 8.8 You are not permitted to run security penetration tests on the Veeam Cloud Connect Services without prior written approval from Rogers. Any such actions will be considered improper use under the Agreement. Rogers may, without liability, restrict Service access if you perform invasive platform testing without prior written approval from Rogers.
- 8.9 If Rogers detects or reasonably believes that your usage represents a security risk, an email will be sent to you, identifying the account(s) affected, and stating that a reinstallation procedure must be performed in order to maintain the integrity of the Instance and the entire infrastructure.
- 8.10 Manipulations consisting of transferring data from the affected system to the new system must be done by you. Rogers will provide reasonable assistance, as determined by Rogers, to you to install a new system but is under no obligation to meet all of your needs in this regard.
- 8.11 Rogers shall not be held responsible for your usage of the Veeam Cloud Connect API by your application.

9 Support

- 9.1 When reporting an incident and creating a ticket for the purposes of technical support, the You agree to provide Rogers with all relevant information reasonably required for the diagnosis and intervention of the incident.
- 9.2 You undertake 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 you to provide Rogers access to your Instance. If you are 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.

10 Software License Grant

- 10.1 Upon purchase of Rogers Veeam Cloud Connect Services by you, Rogers will grant to you a license for Rogers Veeam Cloud Connect. These licenses are subject to and subordinate to the underlying End User License Agreement (EULA) from the Software licensor.
- 10.2 You agree you have read and understood the following:
- 10.2.1 The Services described herein are subject to additional license terms, with which you hereby agree to comply. Your 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](https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms(WW)(ENG)(Apr2014)(CR).pdf)
 - 10.2.2 EULA for VMWare is located here:
https://myaccount.datacentres.rogers.com/legal/vmware_universal_eula.pdf
 - 10.2.3 EULA for Veeam is located here:
<https://myaccount.datacentres.rogers.com/legal/VeeamSoftwareEndUserSoftwareLicenseAgreement.pdf>

- 10.3 Any licenses provided by Rogers to you for your Veeam Cloud Connect Services are solely permitted for use upon the Veeam Cloud Connect infrastructure. Upon termination of the Veeam Cloud Connect Services for any reason, these licenses shall be terminated, and you shall have no further rights to the Software, except as necessary to comply with the Agreement. For greater clarity, “you” in the above paragraph shall also include all End Users.
- 10.4 You will be required to provide your own Veeam Backup & Replication software licensing to be used with the Veeam Cloud Connect platform. You agree that you have taken all necessary steps to ensure that the licenses being used are legally licensed and supported through an agreement between you and the software provider. You will, if required, provide proof of purchase for all your provided licensing being used on the Veeam Cloud Connect platform.
- 10.5 If you make use any non-Rogers provided software, you represent and warrant to Rogers that you have the right and applicable license to use the software in that manner.
- 10.6 If Rogers has agreed to provide management services, then you represent and warrant that your software license agreement with the software provider permits Rogers to perform these activities.
- 10.7 You are responsible for reporting to Rogers any changes to your use of the Services including but not limited to your Veeam Cloud Connect, virtual machines, or software agreements that impact your compliance with any software EULA. If you fail to disclose such changes you are liable for any incremental software licensing fees incurred by Rogers from the time of the change

11 Content

- 11.1 Definition of your Content. Your Content is defined as any software (including machine images), data, text, audio, and video or images that you or any user transfers to Rogers for processing, storage or hosting by the Services in connection with your account and any computational results that you or any user derives from the foregoing through your use of the Services.
- 11.2 Your Content does not include account information. The terms of the Agreement or other agreement with us governing the use of Services apply to Your Content.
- 11.3 Ownership of Content. All interest in and ownership of Content including, but not limited to, those portions of the Content that are your trade names, trademarks or service marks, are and shall remain your property
- 11.4 Rogers is only responsible for maintaining the environment with a level of redundancy in accordance with the Service Level Agreement. This redundancy does not extend to backups of your Content located in the Veeam Backup & Replication.
- 11.5 You shall remove all Content from the Veeam Cloud Connect prior to the date of termination of the Veeam Cloud Connect Services. In the event that the Content is not removed, such Content will be considered abandoned, and Rogers may, without liability to you, delete the Content.
- 11.6 If you have contracted for managed services with Rogers please refer to such other terms.

12. Optional Services

- 12.1 Professional Services. Professional services offered by Rogers to complete your specific requested work are subject to additional charges and require your approval of a Statement of Work. Applicable charges include, but are not limited to travel, living, and miscellaneous expenses. You will also be responsible for all costs associated with the purchase, lease, and/or subscription of any software, hardware or related equipment required to fulfill the Statement of Work.
- 12.2 Data Centre Carrier Neutrality: Rogers will, in its sole discretion, allow third party network and access providers to provide connectivity to your Veeam Cloud Connect Services. Rogers will provision the cross-connection between your colocation space and the third party connectivity provider. You are 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.

13. **Product Service Level Agreement (“SLA”)**

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

Table 1: Power Availability

	Power Availability	Objective	Service Level Credit
Veeam Cloud Connect Availability	Less than 99.99%	<p>Poll Veeam Cloud Connect 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.</p> <p>If the Veeam Cloud Connect 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</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>
MyAccount Portal (MyAccount API and MyAccount Web Portal)	Less than 99.99%	<p>Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN. Impact = 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</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>

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.	<p>Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours</p> <p>Incident Management Resolution Target: Six (6) Hours</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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.	<p>Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours</p> <p>Incident Management Resolution Target: Fourteen (14) Hours</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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.	<p>Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours</p> <p>Incident Management Resolution</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.

		Target: Seventy-two (72) Hours	
Service Request	Response Time Target as indicated below.	<p>Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours</p> <p>Service Request Resolution Target: Five (5) Business Days (Monday to Friday 8am to 8pm EST)</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.
Move/Add/Change/Delete (MACD) Request	Response Time Target as indicated below.	<p>Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours</p> <p>MACD Request Resolution Target: Scoping performed on a case by case basis</p>	SLO Only (no service credit)

13.2 Incident Management Severity Levels:

- 13.2.1 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 your Content is at a significant risk of loss or corruption; You have had a substantial loss of service; and Your business operations have been severely disrupted.
- 13.2.2 Severity 2: Major functionality is severely impaired. High impact; and Degradation of critical service or total of loss non-critical services
- 13.2.3 Severity Level 3 (S3) Partial, non-critical loss of functionality of the Services. Low impact – no direct business impact; and Non-critical services affected;
- 13.2.4 Service Request: A request from you 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).
- 13.2.5 Move/Add/Change/Delete (MACD) Request: Are requests which are ‘add-ons’ or compliment the Veeam Cloud Connect 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.

13.3 Calculation for Response Time and Resolution Target for Incident Management (except if SLO):

- 13.3.1 Response Time Target Rogers response time will be measured from the time you call or create 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 you.
- 13.3.2 Rogers’ resolution will be measured from the time you call or create an Incident ticket in MyAccount Portal (Rogers Support System) to the time a Rogers employee updates the Rogers Support System ticket informing you the incident is resolved.

13.4 Monthly Service Level Credit Limitation. 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.

13.5 Service Credit Request Process. If Rogers has failed to meet any of the above service levels for a particular Site in any given billing month, you 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 you.

13.6 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Veeam Cloud Connect Services. You 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 you will be entitled to as outlined within this SLA.

14. **Termination Fees**

14.1 Except as stipulated in Section 14.3 below, if you terminate the Veeam Cloud Connect Services without cause, or if Rogers terminates the Veeam Cloud Connect Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

- a) fifty (50%) percent of the average monthly charges per terminated Veeam Cloud Connect 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;
- b) one hundred percent (100%) of the non-recurring charges for the terminated Service(s).

14.2 Where you terminate the Veeam Cloud Connect Services prior to the expiration of the Initial Service Term or Renewal Service Term, as applicable, you shall either return all Rogers Equipment associated with the Veeam Cloud Connect Services to Rogers or pay to Rogers the fair market value of such Rogers Equipment.

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

Disaster Recovery as a Service

The following terms pertain specifically to Disaster Recovery as a Service supplied by Rogers to you.

1. 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:

- 1.1 Primary Site – This is the source site for all your 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.
- 1.2 Secondary Failover Site – This is the Rogers hosted target for customer data protected as part of the Rogers Disaster Recovery as a Service. Your content will be copied to this site. This is the location that you will use to restore your content to a working state during a disaster or failover test.
- 1.3 Zerto Virtual Manager (ZVM) – A software plugin for your 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.
- 1.4 Zerto Replication Appliance (VRA) – Software installed into a virtual machine running within your primary virtualized environment responsible for tracking and managing replication between your primary site and the Rogers hosted secondary site.
- 1.5 Zerto User Interface – a GUI used by you to configure, test, and manage the disaster recovery solution, including orchestration of disaster recovery testing and production failover and failback
- 1.6 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 your primary location to participate in the Disaster Recovery as a Service replication and failover orchestration.
- 1.7 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.
- 1.8 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
- 1.9 Zerto Post-Disaster Windows OS Usage – Hourly utilization of virtual machine instances running Microsoft Windows Server
- 1.10 MyAccount Portal – The Rogers portal that you use to manage your user accounts, review billing information, open and review support tickets, purchase additional Services, and review your reporting.
- 1.11 Zerto Replication Storage – Reserved storage resources at the Rogers secondary site supporting the replication of your virtual machines.
- 1.12 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 Recovery event.
- 1.13 VMware vSphere – The virtualized environment on which your Services run is VMware ESXi.
- 1.14 VMware vCloud Director – The VMware portal that presents the Services to you to self-administer. The vCloud Director is the primary tool that you will use to access the post failover Services.
- 1.15 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.
- 1.16 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.
- 1.17 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 you are provided in a separate Statement of Work. Professional Services is required for all sales of the Service.

- 1.18 MS Assisted Disaster Recovery as a Service ("MS Assisted DRaaS") (optional) – Optionally, You 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 your recovery strategy. A completed SOW in the form provided by Rogers and including the details of the services must be completed in writing by You 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).

2 Definitions:

- 2.1 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; your failure to comply with your obligations as defined in the Agreement, including failure to pay valid past-due amounts or any suspension of the Services due to your credit worthiness; failures of your applications or any of your 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 these terms; acts or omissions or any use or user of Disaster Recovery as a Service authorized by you and, or during an event of Force Majeure.
- 2.2 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.
- 2.3 Corporate Support Team - Corporate Support Team means the technical support group at Rogers' responsible for handling all support requests from you. 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.
- 2.4 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 you to use made available to you from within vCloud Director.
- 2.5 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 your Content. Where possible, and if the situation allows for it, you will be notified by Rogers within twenty-four (24) hours of any such Emergency Maintenance.
- 2.6 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 you 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.
- 2.7 Incident Management Resolution – Incident Management Resolution means that the service has been restored as per the SLA and this resolution has communicated to you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.
- 2.8 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.
- 2.9 Move/Add/Change/Delete (MACD) Request – MACD means Your 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.

- 2.10 Organization – Within the vCloud Director, you 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.
- 2.11 Primary Site – Primary Site means the location(s) in which you are responsible for the data centre and compute resources or Rogers through another agreement.
- 2.12 Platform Monitoring and Alarming – The tools used by Rogers to determine the availability of Disaster Recovery as a Service.
- 2.13 Response - measured from the time you call or create an Incident ticket in MyAccount Portal to the time a Rogers employee updates the ticket, speaks to, chats, or emails you.
- 2.14 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.
- 2.15 Scheduled Maintenance - Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected. You shall be given at least five (5) days advance notice of Scheduled maintenance activities. The details of the service window and your negative impact will be communicated to you in the notification.
- 2.16 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 you in the event of a disaster event.
- 2.17 Self-Service – Self Service means any operation carried out by you using an available tool provided by Rogers without submitting a ticket or contacting the Corporate Support Team.
- 2.18 Service Request – Service Request means a request from you 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 you 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.
- 2.19 Service Request Resolution – Service Request Resolution means that the Service Request has been completed and Rogers has communicated this to you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.

3. User Subscriptions types (Standard and Principal)

Access to the Services is configured for two (2) types of users as set out below. Your account will specify the user type. The two available user types are:

- e) **Standard User** – this user level gives a single user the right to access the Disaster Recovery Service and the additional privileges/responsibilities below.
- Access the Zerto User Interface
 - Initiate and Managed a Disaster Recovery test
 - Initiate and manage a disaster recovery event, including failover and failback orchestration
- f) **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:
- Purchasing additional services through the “Buy More” function;
 - Responsible for keeping the account information up to date;
 - Responsible for providing your current contact information for Rogers automatic notification systems;
 - Responsible for receiving all notices from Rogers relating to the Services.

4. Your Responsibilities and Acceptable Use Policy:

- 4.1. You are solely responsible for the creation, management, testing, and execution of your business continuity & disaster recovery plan. You are responsible for declaring a disaster recovery event and ensuring that your technical staff is able to execute on your business continuity & disaster recovery plan using Disaster Recovery as a Service.
- 4.2. You are responsible for configuring, managing, monitoring, and maintaining your primary site's infrastructure, network, software licenses, and applications.
- 4.3. You must grant a Rogers technician or Rogers authorized agent administrator level access to your 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.
- 4.4. You must ensure that your 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 you 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 you performing any changes to your own Primary Site environment or software.
- 4.5. You will not attempt to use the Rogers Failover Site infrastructure as your 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.
- 4.6. You will notify Rogers of any changes to your 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.
- 4.7. You bear all risk associated with your use of the Services.
- 4.8. You are responsible to ensure that the Services are sufficient for your needs.
- 4.9. You are solely responsible to determine that your use of the Services is compliant with all laws and regulations applicable to you.
- 4.10. You agree to use the Services in compliance with all applicable laws and regulations, including, without limitation applicable privacy laws.
- 4.11. You agree not to use the Services:
 - 4.11.1. To violate or infringe on the rights of other customers;
 - 4.11.2. To use the Services to gain unauthorized access to or to disrupt in any manner any third-party service, device, data account or network;
 - 4.11.3. To spam or distribute malware;
 - 4.11.4. In any way that could harm the Services or impair other's users use of the Services;
 - 4.11.5. 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.
- 4.12. To the extent required by applicable laws and your own business requirements, you shall retain connection logs, or any data required to identify any internal or other user of your own services hosted on the Services.
- 4.13. You 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.

- 4.14. You are solely responsible for use of the Services by any individual to whom you may have provided your password(s) and any other means of access (such as SSH access keys, API, etc.).
- 4.15. You are solely liable for the consequences of the loss of any passwords and any other means of access to the Services.
- 4.16. You are responsible for providing appropriate staff to participate in troubleshooting incidents and service requests. During an incident or a service request you will actively participate in the resolution of the request. Any time spent waiting for communications from you may result in the severity of the ticket getting downgraded and the time subtracted from the resolution time.
- 4.17. You are responsible for coordinating all communications with any third party you have contracted to provide any type of support for your services.
- 4.18. You are responsible for maintaining strong password to access the Services. Changes to the access controls require the provision of a You designated secure username and password. Credentials designated by you must utilize strong security traits (e.g. upper and lower case values, numeric and non-numeric values). You are responsible for credentials and must keep credentials secure and confidential.
- 4.19. You shall be solely responsible for providing your services, technical support, pricing and service plans, billing and collections, and any and all other services to your end users, and Rogers shall have no obligations or liability whatsoever to end users in relation to Disaster Recovery as a Service.
- 4.20. You 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. You agree to pay any such charges based on use of the Services by your end users.
- 4.21. In addition to the indemnification provisions set out in the Agreement You 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 you 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.
- 4.22. 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.
- 4.23. Unless Rogers believes an immediate suspension of your Services is required, Rogers will use reasonable efforts to provide notice before suspending your Services.
- 4.24. The Services will continue on a month-to-month basis after the end of the Term with the following conditions:
 - 4.24.1. You are responsible for making end of the Term arrangements by renewing your Services or cancelling the Services.
 - 4.24.2. If you do not make end of Term arrangements then Rogers may, in its sole discretion, terminate the Services.

5. **Your Indemnity.**

In addition to the indemnification provisions set out in the Agreement, you 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 you 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.

- 6.1. The term of each Disaster Recovery as a Service (each an “**Initial Service Term**”) is as set forth in the Agreement(s). These terms commence on the date of signature of the Agreement by You, or, if these terms are attached to the Agreement by way of amendment, then on the date of signature of said amendment by You. Upon expiration of the Initial Service Term, a Disaster Recovery as a Service may be renewed for an additional period set forth in an Agreement 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**”.
- 6.2. The Fees for the Disaster Recovery as a Service, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of Your equipment, Rogers’ equipment or Disaster Recovery as a Service by any third party or unauthorized person.
- 6.3. Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Monthly Recurring Charges set out in any applicable Agreement represent minimum charges. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 6.4. 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 are set out in the Product Quote.
- 6.5. Unless otherwise agreed to in writing by you and Rogers, Rogers reserves the right to commence billing You for the Disaster Recovery as a Service on the earlier of thirty (30) days following execution by you of the Agreement related to the Disaster Recovery as a Service or thirty (30) days after the Service Effective Date in accordance with these terms. 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 your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 6.6. If you purchase 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.
- 6.7. 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 You in the event of an increase in third party supplier costs.
- 6.8. 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.
- 6.9. You must pay invoices within thirty (30) days of the date of each Rogers invoice.

7. Backup, Content Integrity and Disaster Recovery

- 7.1. 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 your Content (defined below) unless otherwise contracted.
- 7.2. Notwithstanding anything to the contrary, the Services do not backup Your Content as part of the Services. You agree to take all the necessary measures to back up your Content in the event of data loss/Content loss or deterioration of Your Content, whatever the cause.

- 7.3. For greater certainty, the inclusion of data replication (as part of resiliency) shall not be considered “data backup” for the purposes hereof.
- 7.4. You are solely responsible to set up your 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. You will access the Services by way of this shared internet connection. If you require private or dedicated network access, you 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 your Disaster Recovery Service. Rogers will provision the cross-connection between your colocation space and the third party connectivity provider. You are 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: You will under no circumstances be permitted to access the physical space or the surrounding facility from which the Services are performed. You 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 your termination for any reason pursuant to the Agreement.
- 8.5. Fair Use of the Services: The Services are subject to fair use by you. Rogers will ensure that you do not disrupt the use of other users of the Services. Rogers will prevent Noisy Neighbours and will generally limit the ability of you to adversely affect other users and other Customers. Noisy Neighbor means you 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 you are a Noisy Neighbour Rogers may, and Rogers reserves the right to temporarily limit your use of the Services. Rogers will attempt to contact you prior to any corrective action. Any action by Rogers to address a Noisy Neighbour and any disruption to your Services is excluded from the SLA for the Services.
- 8.6. Client Side Internet: You will access the Services remotely via the internet. You must have your 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: You 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.**
- 9.1. You agree to implement and is wholly responsible for implementing reasonable security precautions and practices in relation to the use of Disaster Recovery as a Service.
- 9.2. You are solely responsible for any non-physical security breach or unauthorized usage of Disaster Recovery as a Service.
- 9.3. 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.

- 9.4. You are solely responsible for user access security or network access security with respect to your Content.
- 9.5. 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.
- 9.6. You are 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. You are responsible for any use of the account regardless of who uses the Services.
- 9.7. Rogers will track all access to your Services through the online ticketing system/support system and will ensure that you have all your necessary documented approvals prior to accessing or changing your Services. If Rogers cannot verify your 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.
- 9.8. When a situation is considered a security breach or could have serious consequences, Rogers will notify you and will act on your behalf if Rogers is unable to get correct approvals in a timely manner to deal with the threat.
- 9.9. 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.
- 9.10. You agree to co-operate and assist Rogers with any investigation or action taken in relation to Rogers' operations and provisioning of services, confirmation of your compliance with the Agreement and, or breach of the Agreement by you.
- 9.11. 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. You 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.
- 9.12. You are 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 You performs invasive platform testing without written approval.
- 9.13. To the extent practicable, updates are performed in collaboration with You. For any avoidance of doubt, after the delivery of the Service to you, the responsibility to manage and update of the operating systems and pre-installed applications is transferred to you.
- 9.14. Notwithstanding the foregoing, Rogers reserves the right to request that you install updates and patches in connection to running Services. If you fail 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 your Content or the Services or to Rogers, its Subcontractors, or other customers, Rogers may suspend access to the Service(s) until you comply with such request or the Service is reinstalled.
- 9.15. If Rogers detects or reasonably believes that your usage represents a security risk, an email will be sent to you, 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.
- 9.16. In case of a security breach Rogers reserves the right to suspend the Services immediately in order to maintain the integrity of your Content.

9.17. 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 your data/Content, or (b) your 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. You acknowledge that such suspensions do not release it of any obligation to pay for the Services.

9.18. Rogers shall not be held responsible for your usage of the Disaster Recovery as a Service, notably for any misuse of the Services by you through the Self Service Portal.

10. Support

10.1. When reporting an incident and creating a ticket for the purposes of technical support, you agree to provide Rogers with all relevant information reasonably required for the diagnosis and intervention of the incident.

10.2. You undertake 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 you to provide Rogers access to its Service. If you are 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

11.1. Upon purchase of Disaster Recovery as a Service by You, Rogers will grant to You 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.

11.2. You agree you have read, understood, and agreed to the following EULA's if making use of any such services:

11.2.1. The Services described herein are subject to additional license terms, with which you hereby agree to comply. Your 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](https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms(WW)(ENG)(Apr2014)(CR).pdf)

11.2.2. EULA for VMWare is located here:

https://myaccount.datacentres.rogers.com/legal/vmware_universal_eula.pdf

11.2.3. EULA for Redhat is located here:

https://myaccount.datacentres.rogers.com/legal/GLOBAL_EULA_RHEL_English_20101110.pdf

11.2.4. EULA for Zerto is located here:

<https://myaccount.datacentres.rogers.com/legal/ZertoEndUserLicenseAgreement.pdf>

11.3. Any licenses provided by Rogers to you 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 You shall have no further rights to the Software, except as necessary to comply with the Agreement. For greater clarity, "you" in the above paragraph shall also include all end users.

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

11.5. If you makes use any non-Rogers provided software, you represent and warrant to Rogers that you have the right and applicable license to use the software in that manner.

- 11.6. If Rogers has agreed to provide management services, then you represent and warrant that your software license agreement with the software provider permits Rogers to perform these activities.
- 11.7. You are responsible for reporting to Rogers any changes to your use of the Services including but not limited to Disaster Recovery as a Service, virtual machines, or software agreements that impact your compliance with any software EULA. If you fail to disclose such changes you are liable for any incremental software licensing fees incurred by Rogers from the time of the change.

12. **Content**

- 12.1. Definition of Your Content. Your Content is defined as any software (including machine images), data, text, audio, and video or images that you or any user transfers to Rogers for processing, storage or hosting by the Services in connection with your account and any computational results that you or any user derives from the foregoing through your use of the Services.
- 12.2. Your Content does not include account information. The terms of the Agreement or other agreement with us governing the use of Services apply to your Content.
- 12.3. Ownership of Content. All interest in and ownership of Content including, but not limited to, those portions of the Content that are Your trade names, trademarks or service marks, are and shall remain the property of you
- 12.4. 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 Your Content located within Disaster Recovery as a Service.
- 12.5. You 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 you, delete the Content.
- 12.6. When evaluating the security of a cloud solution, it is important for you to understand and distinguish between the following:
- 12.6.1. 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.
 - 12.6.2. Your responsibility is determined by the services that you have contracted for with Rogers. If you contract for a Rogers cloud service, you are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by you in the cloud service, and the configuration of any Rogers-provided firewall.
- 12.7. If you have contracted for managed services with Rogers please refer to such other terms.

13. **Product Service Level Agreement (“SLA”)**

- 13.1. If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you 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	99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month. Less than 99.85% Monthly = Rogers will issue a credit

		<p>following calculation:</p> $\text{Impact} = \text{SUM}(\text{DOWN_POLL})$ $\text{Deviation} = \text{Total time available in the Month in Min.} - \text{Impact}$ $\text{Availability} = \text{Deviation} / \text{Total time available in the Month in Min.} \times 100$	to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.
MyAccount Portal (MyAccount API and MyAccount Web Portal)	99.99%	<p>Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN.</p> $\text{Impact} = \text{SUM}(\text{DOWN_POLL})$ $\text{Deviation} = \text{Total time available in the Calendar Month in Min.} - \text{Impact}$ $\text{Availability} = \text{Deviation} / \text{Total time available in the Month in Min.} \times 100$	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>
Zerto Service Portals (Zerto dedicated vCloud Director and Zerto Management Portal (Cloud Based))	99.99%	<p>Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN.</p> $\text{Impact} = \text{SUM}(\text{DOWN_POLL})$ $\text{Deviation} = \text{Total time available in the Calendar Month in Min.} - \text{Impact}$ $\text{Availability} = \text{Deviation} / \text{Total time available in the Month in Min.} \times 100$	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>

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

		Five (5) Business Days (Monday to Friday 8am to 8pm EST)	
MOP Service Request	Response Time Target as indicated below.	Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Six (6) Hours	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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 you call in live 24x7 = Live answer When you create 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)

13.2. Incident Management Severity Levels (Table 2):

- 13.2.1. 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 your Content is at a significant risk of loss or corruption; you have had a substantial loss of service; and your business operations have been severely disrupted.
- 13.2.2. Severity 2: Major functionality is severely impaired. High impact; and Degradation of critical service or total of loss non-critical services
- 13.2.3. Severity Level 3 (S3) Partial, non-critical loss of functionality of the Services. Low impact – no direct business impact; and Non-critical services affected;
- 13.2.4. Service Request: A request from you 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).
- 13.2.5. 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.

13.3. Calculation for Response Time and Resolution Target (Table 2) for Incident Management (except if SLO):

- 13.3.1. Response Time Target Rogers response time will be measured from the time you call or create 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 you.
- 13.3.2. Rogers' resolution will be measured from the time you call or create an Incident ticket in MyAccount Portal (Rogers Support System) to the time a Rogers employee updates the Rogers Support System ticket informing you the incident is resolved.

13.4. Monthly Service Level Credit Limitation. 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.

13.5. Service Credit Request Process. If Rogers has failed to meet any of the above service levels for a particular Site in any given billing month, you 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 you.

- 13.6. Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Disaster Recovery as a Service. You 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 you will be entitled to as outlined within this SLA.

14. Termination Fees

- 14.1. If you terminate the Services without cause, or if Rogers terminates the Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:
- a) 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;
 - b) all usage, taxes, and late payment charges incurred up to the date of termination; and
 - c) one hundred percent (100%) of the non-recurring charges for the terminated Service(s).
- 14.2. Where you terminate the Services prior to the expiration of the Initial Service Term or Renewal Service Term, as applicable, you shall either return all Rogers Equipment associated with the Services to Rogers or pay to Rogers the fair market value of such Rogers Equipment.
- 14.3. The above shall be included in an invoice to you subsequent to termination.to you subsequent to termination.

Managed Private Cloud Services

The following terms pertain specifically to Managed Private Cloud Services supplied by Rogers to you.

Managed Private Cloud Service(s) ("**Services**") are based on the written requirements provided to Rogers by you. The Managed Private Cloud Services are made up of a combination of physical compute (CPU/RAM) nodes and storage, over the top of which a virtualization environment using VMWare vSphere is deployed.

1. **Definitions.** Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:
 - 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; your failure to comply with your obligations as defined in these terms and in the Agreement, including failure to pay valid past-due amounts or any suspension of the Services due to your credit worthiness; failures of your applications or any of your 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 these terms; acts or omissions of you or any use or user of the Managed Private Cloud Services authorized by you; 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. Compute Availability - Rogers will use its Platform Monitoring and Alarming system to poll the availability of each type of Compute. Compute means the vCPU and vRAM resources available to you.
 - 1.4. Corporate Support Team - Corporate Support Team means the technical support group at Rogers' responsible for handling all support requests from you. 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.
 - 1.5. Colocated Site means the physical Rogers data centre location in which Space for your equipment is made available by Rogers, as specified in the attached Agreement(s).
 - 1.6. Emergency Maintenance – Emergency Maintenance means any maintenance activities performed to prevent potential failures to infrastructure on which the Services are connected or to avoid a security breach that could compromise your Content. Where possible, and if the situation allows for it, you will be notified by Rogers within twenty-four (24) hours of any such Emergency Maintenance.
 - 1.7. Host – The physical server on which the virtual machines reside.
 - 1.8. Incident Management – An Incident means an unplanned interruption to any part of the Managed Private Cloud Service or reduction in the quality of the Managed Private Cloud Service. An Incident can be created by you 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.
 - 1.9. Incident Management Resolution – Incident Management Resolution means that the Services have been restored as per the SLA and this resolution has been communicated to you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.
 - 1.10. Move/Add/Change/Delete (MACD) Request – MACD means your requests which are 'add-ons', changes or compliment the Managed Private Cloud 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.

- 1.11. Network - Network means the TCP/IP-based data communications network (including all hardware, software, telecommunications facilities and equipment) owned and operated by Rogers.
- 1.12. Out of Service Condition means a condition whereby there is a Managed Private Cloud Service outage, including any lack of Managed Private Cloud Availability.
- 1.13. Platform Monitoring and Alarming – The tools used by Rogers to determine the availability of the Managed Private Cloud Service.
- 1.14. Response - measured from the time you call or create an Incident ticket in MyAccount Portal to the time a Rogers employee updates the ticket, speaks to, chats, or emails you.
- 1.15. Rogers Support System - The tools used by Rogers to record and track all Service Requests and Incidents Requests as part of the Managed Private Cloud Service.
- 1.16. Scheduled Maintenance - Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected. You shall be given at least five (5) days advance notice of Scheduled Maintenance activities. The details of the service window and any negative on your Services will be communicated to you in the notification.
- 1.17. Self-Service – Self Service means any operation carried out by you 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 you 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 you 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 you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.
- 1.20. Space means a designated section of the Colocated Site where space of one or more equipment cabinets (or racks) are set-aside by Rogers for your equipment.
- 1.21. Virtual Data Centre - Virtual Data Centre (VDC) is made up of the equipment and storage space dedicated to your Managed Private Cloud Services.
- 1.22. Virtual Machine – The software representation of a computer system running on top of VMware vSphere.

2. Features. Rogers Managed Private Cloud Services have the following features:

- 2.1 Compute Nodes – each Managed Private Cloud Services environment is configured with the required amount of Physical CPU and RAM. Where N+1 (redundant hardware) is required, this must be outlined as a requirement in a Statement of Work.
- 2.2 Storage - Your storage capacity is allotted increments of 1 Gigabyte (1 GB = 1000000000 bytes (= 1000³ Bytes)). Storage is characterized in three ways as set out below. Selection of the storage device and its configuration can have an impact on the usable storage. Rogers will provide the available Raw Storage (based on the physical attributes of the device) and the Effective Storage (based on industry standards and information provided by you) to the you. Usable Storage is a result of many factors and will change depending on your communicated requirements, selections, and overtime based on usage. Definitions are as set out below:
 - 2.2.1 Raw Storage: This is the physical storage provided without the use of any compression or de-duplication. Raw Storage is calculated by adding up the capacity of all the physical storage in the device.

- 2.2.2 Effective Storage: This represents how much storage is presented after advanced compression and deduplication is applied to the Raw Storage. The compression and de-duplication technologies can increase the available storage by multiples and is expressed in the form of a ratio. 1:1 means no increase, 2:1 means double the Raw Storage, 3:1 means triple the Raw Storage and so on. This ratio is not guaranteed, and changes depending on the types of content being written to the storage.
- 2.2.3 Usable Storage: This represents the amount of storage available for you to store your content. To calculate the Usable Storage, subtract all overhead for the Managed Private Cloud from the Effective Storage.
- 2.3 Network – the Managed Private Cloud Services will utilize a Cisco 10Gb network switch. A minimum of (2) two switches are required to ensure availability. The number of your usable ports is dependent on the number of ports used to assemble the private cloud.
- 2.4 Infrastructure Monitoring and Alarming – the infrastructure supporting the Managed Private Cloud Services is managed by Rogers. Management of the Managed Private Cloud infrastructure, physical hosts, switching and storage includes: 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 as provided by installed agent), issue identification and remediation; and SLA statistics. All features are configured and supported by Rogers.
- 2.5 MyAccount Portal – The Rogers portal that you use to manage your user accounts, review billing information, open and review support tickets, purchase additional Services, and review your reporting.
- 2.6 Hypervisor Monitoring and Alarming – the Hypervisor supporting the Managed Private Cloud Services is managed by Rogers. Hypervisor management includes: Threshold alerting (Configuration of alerts based on sustained capacity usage and industry standards), Quarterly Reports (Usage reports CPU, RAM, Drives, Uptime, trending, capacity planning), Issue identification and remediation, Patching; and SLA statistics. All features are configured and supported by Rogers.
- 2.7 Infrastructure Refresh – equipment manufacturer guarantees, warranties and service agreements are purchased by Rogers to be co-terminus with the Initial Service Term for the Managed Private Cloud Services. Infrastructure refresh is provided upon the latter of the expiry of the equipment manufacturer's warranty and your commitment to a new Service Term for Managed Private Cloud Services.
- 2.8 Linux based OS – Subscriptions of Red Hat Enterprise Linux (RHEL) are available. RHEL subscription are governed by the End User License Agreement described below.
- 2.9 Microsoft based OS and Application Software – Subscriptions to a large variety of Microsoft Server OS and Applications are available. All Microsoft subscriptions are governed by your End User License Agreements as described below.
- 2.10 Professional Services - The standard installation charges for each component of the Managed Private Cloud Services are set out in the Agreement. Where your requests custom configuration of the Managed Private Cloud Services beyond standard installation, Rogers will quote such configuration as Professional Services to you in a separate Statement of Work.
- 2.11 (Optional) Hypervisor Self-Management – If requested, Rogers will configure a permission type on the Hypervisor that allows you to perform basic functions related to turn up of your own virtual machines and some settings related to that action. Rogers has, in its sole discretion, defined the permission types made available for you to use.
- 2.12 Additional Managed Server per virtual machine – These services are only available if you have contracted for such Managed Service separate from these terms. Three tiers of services are available as set out below:
 - 2.12.1 Fully Managed services – A service level where you have elected to have the Services operated, maintained, monitored and patched by Rogers for a monthly fee and a one-time setup cost.

- 2.12.2 Proactive Monitoring/Patching/Reporting services – A service level where you have elected to have the virtual machines maintained, monitored, and patched by Rogers for a monthly fee and a one-time setup cost.
- 2.12.3 Self-Serve Monitoring and Alerting – A service level where you have elected to have the virtual machines monitoring enabled and transmitted to you by Rogers for a monthly fee and a one-time setup cost.

2.13 Additional Managed Backup per virtual machine – These services are only available if you have contracted for Managed Backup Services separate from these terms. The Managed Backup Services consist of one tier of services as set out below:

- 2.13.1 Fully Managed Backup – A service level where you have elected to have the Services backed up by Rogers for a monthly fee and a one-time setup cost.

3. User Subscription types (Standard and Principal)

Access to the Services is configured for two (2) types of users as set out below. Your account will specify the user type. The two available user types are:

- g) **Standard User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below.
 - Use of the Managed Private Cloud Services resources.
- h) **Principal User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below:
 - Purchasing additional services through the “Buy More” function;
 - Adding Standard Users to the Services;
 - Responsible for keeping the account information up to date;
 - Responsible for providing your current contact information for Rogers automatic notification systems; and
 - Responsible for receiving all notices from Rogers relating to the Services.

4. Your Responsibilities and Acceptable Use Policy:

- 4.1 You bear all risk associated with your use of the Services.
- 4.2 You are responsible to ensure that the Services are sufficient for your needs.
- 4.3 You are solely responsible to determine that your use of the Services is compliant with all laws and regulations applicable to you.
- 4.4 You agree to use the Services in compliance with all applicable laws and regulations, including, without limitation applicable privacy laws.
- 4.5 You agree not to use the Services:
 - 4.5.1 To violate or infringe on the rights of other customers;
 - 4.5.2 To use the Services to gain unauthorized access to or to disrupt in any manner any third-party service, device, data account or network;
 - 4.5.3 To spam or distribute malware;
 - 4.5.4 In any way that could harm the Services or impair other’s users use of the Services;
 - 4.5.5 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.
- 4.6 To the extent required by applicable laws and your own business requirements, you shall retain connection logs, or any data required to identify any internal or other user of your own services hosted on the Services.
- 4.7 You 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.
- 4.8 You are solely responsible for use of the Services by any user to whom you may have provided your password(s) and any other means of access (such as SSH access keys, API, etc.).

- 4.9 You are solely liable for the consequences of the loss of any passwords and any other means of access to the Services.
- 4.10 You are responsible for providing appropriate staff to participate in troubleshooting incidents and service requests. During an incident or a service request you will actively participate in the resolution of the request. Any time spent waiting for communications from you may result in the severity of the ticket getting downgraded and any such time will be subtracted from the resolution time.
- 4.11 You are responsible for coordinating all communications with any third party you have contracted to provide any type of support for your Services.
- 4.12 You access the Services via the Wide Access Network (WAN). You must have a WAN connection to access the Service, and is solely responsible for the aforementioned WAN connection, in particular your availability, reliability and security.
- 4.13 You are responsible for maintaining strong passwords to access the Services. Changes to the access controls require the provision of your designated secure username and password. Credentials designated by you must utilize strong security traits (e.g., upper and lower case values, numeric and non-numeric values). You are responsible for all access credentials and agree to keep credentials secure and confidential.
- 4.14 You shall be solely responsible for providing your services, technical support, pricing and service plans, billing and collections, and any and all other services to your end users, and Rogers shall have no obligations or liability whatsoever to your end users in relation to the Managed Private Cloud Services.
- 4.15 You will inform all your end users of any terms and conditions and any associated costs including any potential charges, overages, and other fees associated with the Services. You agree to pay any such charges based on use of the Services by your end users.
- 4.16 Violation of the terms in this section may result in suspension of the Service. Rogers may, at its sole discretion, suspend the Services as it deems necessary.
- 4.17 Unless Rogers believes an immediate suspension of your Services is required, Rogers will use reasonable efforts to provide notice to you before suspending your Services.
- 4.18 The Services will continue on a month-to-month basis after the end of the Service Term with the following conditions:
 - 4.18.1 You are responsible for making end of the Service Term arrangements by renewing your Services or cancelling the Services.
 - 4.18.2 If you do not make end of the Service Term arrangements then Rogers may, in its sole discretion, terminate the Services in accordance with the terms of the Agreement.
- 4.19 Your Hypervisor Self-Management (if requested by you) – Rogers will provide you with credentials with the associated permissions to perform basic Hypervisor actions related to the creation of virtual machines and some of the settings around that process. You accept the following additional responsibilities when making use of this ability, rather than having the work performed by Rogers staff:
 - 4.19.1 You are responsible for using your own change management process to track any changes made in the environment. Rogers will not actively track these changes nor provide any roll back capabilities.
 - 4.19.2 There is a risk associated with over-provisioning your storage. You accept full responsibility for capacity management of the storage allocated to you and any issues that may arise from your misconfiguration and/or over-provisioning including but not limited to, loss of data, virtual machine downtime, and any impact on the performance of any part of the Services and the SLA's or Service level objectives (the "SLO's") contained in this document.
 - 4.19.3 There is a risk associated with over provisioning your vCPU and vRAM. You accept the full responsibility for capacity management of the compute and memory allocated to them and issues that may arise from your misconfiguration and/or over-provisioning including but not

limited to loss of data, virtual machine downtime, and any impact on the performance of any part of the Services and the SLA's or SLO's contained in this document.

- 4.19.4 There is a risk associated with the incorrect configuration of any Hypervisor setting. You accept full responsibility for any changes you make to the environment. You also accept responsibility for any issues that may arise from your misconfiguration and/or over-provisioning including but not limited to loss of data, virtual machine downtime, and any other impact on the performance of any part of the Services and the SLA's or SLO's contained in this document.
- 4.19.5 There is a risk associated with you deleting data, settings or virtual machines from the Hypervisor. You accept the full responsibility for any data, settings or virtual machines they delete. You accept all responsibility for any issues that may arise from your misconfiguration and/or over-provisioning including but not limited to loss of data, virtual machine downtime, and any impact on the performance of any part of the Services and the SLA's or SLO's contained in this document.

5 **Your Indemnity.**

In addition to the indemnification provisions set out in the Agreement, you 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 arising (i) from or for any third-party intellectual property rights, for which you agree to lawfully obtain any licences required, if any, to use any third-party intellectual property, including software; (ii) from or for the use of any third-party licenses including but not limited to, Microsoft, Red Hat, and Oracle, and (iii) from or for the use of any third-party content.

6 **Term, Rates, and Charges.**

- 6.1 The term of each Managed Private Cloud Service (each an “**Initial Service Term**”) is as set forth in the Agreement(s). The term of this Schedule commences on the date of signature of the Agreement by you, or, if this Schedule is attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon expiration of the Initial Service Term, a Managed Private Cloud Service may be renewed for an additional period set forth in an Agreement to be added to this Agreement by way of amendment (a “**Renewal Service Term**”) or, if no amendment is executed, the Managed Private Cloud 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**”.
- 6.2 The Fees for the Managed Private Cloud Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Unless otherwise specified, there are no limits or restrictions on usage. Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Managed Private Cloud Services by any third party or unauthorized person.
- 6.3 Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 6.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Managed Private Cloud Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Managed Private Cloud Services 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 your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 6.5 Rogers may charge you additional charges arising from the use of software, including but not limited to Microsoft Service Provider Licensing (SPLA) and VMware (VCP). This applies to such software and all consumption-based license models. The use of such software by you will be calculated as overages by Rogers and added to your invoice. Such invoicing is prorated from the time the overage begins. You will be invoiced continuously until you are no longer using overage and/or your use is reduced to the contracted

amount. Your standard billing will be reflected starting on your first bill after the overage. Refer to Section 11 for additional information related to the terms and conditions of use of SPLA and VCPP.

- 6.6 Rogers reserves the right to change rates for any and all Managed Private Cloud Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.
- 6.7 Upon the commencement of a Month-to-Month Renewal Term for a Managed Private Cloud Service, the rates for such Managed Private Cloud Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 6.8 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

7 Backup, Content Integrity, and Disaster Recover

- 7.1 Set-up and Maintenance - Backup Services. If you have not purchased Cloud Backup Managed Services, Rogers is not responsible to you for providing, or for any cost or expenses associated with providing, any administrative, technical, emergency or support personnel associated with the Managed Private Cloud Services or for providing and maintaining the Content on the Managed Private Cloud.
- 7.2 Notwithstanding anything to the contrary, the Services do not backup your specific data on the Instances, Storage or Object Storage Containers. It is therefore the responsibility of you to take all the necessary measures to back up your data in the event of data loss or deterioration of entrusted data, whatever the cause, including causes not expressly mentioned in this document or the Agreement.
- 7.3 Rogers does not provide any guarantees related to your data loss prevention. For greater certainty, the inclusion of data replication (as part of resiliency) shall not be considered "data backup" for the purposes hereof.
- 7.4 You are solely responsible to set up your own business continuity plan and/or business recovery plan, notably when the Services are used for the purpose of hosting sensitive data necessary for your respective activities. It is recommended that you create a back-up of your data in two (2) or more different and geographically distant data centres in order to prevent against any event which may impact the availability, integrity and/or confidentiality of your data.

8 Services and Networking.

- 8.1 Set-up and Maintenance. If you have not purchased Cloud Backup Managed Services, Rogers is not responsible to you for providing, or for any cost or expenses associated with providing, any administrative, technical, emergency or support personnel associated with the Managed Private Cloud Services or for providing and maintaining the Content on the Virtual Data Centre. Rogers is responsible for maintaining the Virtual Data Centre.

If you are co-managing your own Managed Private Cloud Services, they will be permitted to turn up and take down virtual server instances as required. If you provision a virtual server instance and it is determined that the virtual server is unaligned, you will have a period of two (2) weeks to correct the action by aligning the virtual server or Rogers will, without liability, suspend that specific virtual server.

- 8.2 Domain Name and Network Number. You will arrange the required domain name service (DNS) for any Services that you desire to be accessible by hostname over the Internet. Rogers will, upon your request, provide DNS with a Service only if it is contracted to provide your network access to a Service. You are responsible for all charges for DNS provided by Rogers.

You may use a domain name or subdomain name that is already registered under your business name. You shall be solely responsible for any domain registration fees, maintenance fees and taxes incurred in connection with your domain names. You may also use Rogers provided DNS services, subject to applicable Rogers' charges.

You shall arrange for the provision of domain name service (DNS) for any Managed Private Cloud Services you desire to be accessible by hostname over the Internet, or, at your option, you may request that Rogers provide such Domain Name Services only to the extent necessary to provide such access to the Managed Private Cloud Services, in which case such Domain Name Services will be set out in an Agreement and described in an applicable Product Schedule. You may use a domain name or subdomain already registered under your business name. You shall be solely responsible for the domain registration fees and maintenance taxes incurred in connection with each new domain name. Rogers shall supply to you (subject to reasonable availability) and route a number of Classless Inter-Domain Routing (CIDR) host Internet Protocol (IP) addresses from its allocation of addresses to support Network access to the Managed Private Cloud Services. Such IP addresses are provided to you pursuant to the terms of the IP Address Policy, available at www.rogers/terms.

- 8.3 **Responsibility for End Users.** You shall be solely responsible for providing your services, technical support, pricing and service plans, billing and collections, and any and all other services to your End Users, and Rogers shall have no obligations or liability whatsoever to End Users in relation to the Managed Private Cloud Services.
- 8.4 **Ownership of Private Cloud.** You will in no case be permitted to access the physical space or the surrounding facility from which the Managed Private Cloud Services are performed. You will not acquire any interest in, nor file any liens upon, the Data Centre, the Rogers Equipment, any portion of the data centre as a result of the provision by Rogers of the Managed Private Cloud Services or their termination for any reason pursuant to the Agreement.

9 Security Access and Fraud.

- 9.1 You agree to implement and are solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Managed Private Cloud Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Managed Private Cloud Services, your equipment, including unmanaged Rogers equipment, and your accounts.
- 9.2 Rogers shall use commercially reasonable efforts to prevent unauthorized access to Managed Private Cloud Services. Where a situation is considered a security breach, Rogers shall notify you as soon as feasible and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 9.3 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, Services and/or your data, or (b) your breach of the Agreement. In case of a security breach Rogers reserves the right to suspend the Services immediately in order to maintain the integrity of your Content. 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. You acknowledge that such suspensions do not release you of any obligation to pay for Services.
- 9.4 You are solely responsible for user access security or network access security with respect to your Content.
- 9.5 Rogers will track all access to your Services through an online ticketing system and ensure that those who requested access have all your necessary documented approvals prior to accessing or changing your Managed Private Cloud Services.
- 9.6 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.
- 9.7 In the event of any emergency that presents a risk of service outage, or damage to Rogers' equipment or data belonging to Rogers, a third party, the Site or Rogers' data centre facilities, or to any persons or property present therein, Rogers may disable Managed Private Cloud Services as is reasonably necessary to respond to the emergency.

- 9.8 All Content within the Virtual Data Centre is completely isolated through the use of industry standard virtualization protocols and VLAN rules within the infrastructure. You are further isolated with virtual firewalls. All Content will be located within the Virtual Data Centre which is housed within one of Rogers' data centre facilities located within Canada.
- 9.9 You are not permitted to run security penetration tests on the Managed Private Cloud Services 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 you perform invasive platform testing without Rogers written approval.
- 9.10 To maintain the level of security for your Services, Rogers may update the operating systems before pre-installing them on the Services. You acknowledge that ensuring the level of security may cause an impact on your use of the Services. Notwithstanding the foregoing, Rogers shall use commercially reasonable efforts to avoid material impact on the functionality of the Services, subject to patches of third party products, which Rogers does not control.
- 9.11 To the extent practicable, updates are performed in collaboration with you. For any avoidance of doubt, after the delivery of the Service to you, the responsibility to manage and update of the operating systems and pre-installed applications is transferred to you.
- 9.12 Notwithstanding the foregoing, Rogers reserves the right to request that you install updates and patches in connection to running Services. If you fail 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 your Content or the Services or to Rogers, its Subcontractors, or other customers, Rogers may suspend access to the Service(s) until you comply with such request, or the Service is reinstalled.
- 9.13 If Rogers detects or reasonably believes that your usage represents a security risk, an email will be sent to you, 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. In such a case, Rogers reserves the right to suspend the Services immediately in order to maintain the integrity of your Content.
- 9.14 Manipulations consisting of transferring data from the affected system to the new system must be done by you. Rogers will provide reasonable assistance to you to install a new system but is under no obligation to meet all of your needs in this regard.
- 9.15 Rogers shall not be held responsible for your usage of the VMware vCloud Director API, notably for any misuse of the Services by you through the API.
- 9.16 Hypervisor Self-Management – Rogers solely has defined the permission type made available for you to use. Rogers may change the type of permissions made available to you at any time.

10 Support

- 10.1 When reporting an incident and creating a ticket for the purposes of technical support, you agree to provide Rogers with all relevant information reasonably required for the diagnosis and intervention of the incident.
- 10.2 You undertake 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 you to provide Rogers access to your Service. If you are 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

- 11.1 Upon purchase of Managed Private Cloud Services by you, Rogers will grant to you a license for Virtual Data Centre operating systems (OS) and associated Software. These licenses are subject to and subordinate to the underlying End User License Agreement (EULA) from the OS or Software licensor.

11.2 You agree they have read and understood the following EULA's if making use of any such services:

11.2.1 The Services described herein are subject to additional license terms, with which you hereby agree to comply. Your 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](https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms(WW)(ENG)(Apr2014)(CR).pdf)

11.2.2 EULA for VMWare and VCPP is located here:
https://myaccount.datacentres.rogers.com/legal/vmware_universal_eula.pdf

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

11.3 Any licenses provided by Rogers to you for the Managed Private Cloud Services are solely permitted for use upon the Virtual Data Centre infrastructure. Upon termination of the Managed Private Cloud Services for any reason, these licenses shall be terminated, and you shall have no further rights to the Software, except as necessary to comply with the Agreement. For greater clarity, "you" in the above paragraph shall also include all end users.

11.4 You agree that, in the event you provide your own software licenses, you have taken all necessary steps to ensure that the software licenses being used are legally licensed and supported through a valid agreement between you and the software provider. You will, if required by Rogers, provide proof of purchase for all your provided software being used on the Private Cloud platform. You may not, under any circumstances, provide your own Microsoft Windows licenses. Your provided Microsoft Windows licenses are prohibited in the Microsoft EULA listed in this document.

11.5 If you make use any non-Rogers provided software, you represent and warrants to Rogers that you have the right and applicable license to use the software in that manner.

11.6 If Rogers has agreed to provide management services, then you represent and warrants that your software license agreement with the software provider permits Rogers to perform these activities

11.7 You are responsible for reporting to Rogers any changes to your use of the Services including but not limited to the Private Cloud, virtual machines, or software agreements that impact your compliance with any software EULA. If you fail to disclose such changes you are liable for any incremental software licensing fees incurred by Rogers from the time of the change.

12 **Content**

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

12.2 Your Content does not include account information. The terms of the Agreement or other agreement with us governing the use of Services apply to your Content.

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

12.4 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 your Content located in the Private Cloud.

12.5 You shall remove all Content from the Virtual Data Centre prior to the date of termination of the Managed Private Cloud Services. In the event that the Content is not removed, such Content will be considered abandoned, and Rogers may, without liability to you, delete the Content.

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

- 12.6.1 Rogers is responsible for protecting the infrastructure that runs all the services offered as part of the Services. This infrastructure is composed of the hardware, software, networking, and facilities that run the Services.
- 12.6.2 Your responsibility is determined by the services that you have contracted for with Rogers. If your 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 you in the cloud service, and the configuration of any Rogers-provided firewall.

13 Optional Services

13.1 Network Access. Where requested by you, Rogers will provide network access to the Managed Private Cloud Services. Except for such network access and remote console access provided exclusively for operational purposes, any form of connectivity between the Rogers Equipment on which the Managed Private Cloud Services are hosted and any network or transmission medium other than Rogers is prohibited. If you exceed the transfer limits set out in the Agreement, overage charges will apply. There are no restrictions in place that will limit network usage and you will be held responsible for all usage, including any resulting from network abuse or attack. Such network access will be provided in accordance with these terms for Data Centre Access.

13.2 Data Centre Carrier Neutrality. Rogers will, in its sole discretion, allow third party network and access providers to provide connectivity to your Managed Private Cloud Services. Rogers will provision the cross-connection between the Space and the third party connectivity provider. You are 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.

14 Product Service Level Agreement ("SLA")

14.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("**Service Credit**").

Table 1: Availability

	Monthly Objective	Calculation	Service Level Credit
Compute Availability (where Hypervisor is used)	99.99%	<p>The Rogers Platform Monitoring and Alarming system performs the following:</p> <p>Poll each host's management network adapters every 5 min. If Host Maintenance Mode = False AND connectivity to the physical network records a value of DOWN (100% Loss TX or RX), OR all physical hosts power supplies = OFF AND Service Window = False, then record Compute = DOWN.</p> <p>If the Host is DOWN perform the following calculation:</p> <p>Impact = SUM(HOST_DOWN_POLL) Deviation = Total time available in the month in Min. – Impact Availability = Deviation / Total time available in the month in Min. X 100</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>

Network Availability (where Hypervisor is used)	99.99%	<p>The Rogers Platform Monitoring and Alarming system performs the following:</p> <p>Poll each host's network adapter every 5 min. If Host Maintenance Mode = False AND host connectivity to the physical network records a value of DOWN (100% Loss TX or RX) then record Network = DOWN.</p> <p>Impact = SUM(DOWN_POLL)</p> <p>Deviation = Total time available in the month in Min. – Impact</p> <p>Availability = Deviation / Total time available in the month in Min. X 100</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>
Storage Availability	99.99%	<p>Poll Managed Private Cloud 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.</p> <p>If the Managed Private Cloud Gateway is DOWN perform the following calculation:</p> <p>Impact = SUM(DOWN_POLL)</p> <p>Deviation = Total time available in the Month in Min. – Impact</p> <p>Availability = Deviation / Total time available in the Month in Min. X 100</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>
MyAccount Portal (MyAccount API and MyAccount Web Portal)	99.99%	<p>Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN.</p> <p>Impact = SUM(DOWN_POLL)</p> <p>Deviation = Total time available in the Calendar Month in Min. – Impact</p> <p>Availability = Deviation / Total time available in the Month in Min. X 100</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>

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.	<p>Response Target Metric:</p> <p>When you call in live 24x7 = Live answer</p> <p>When you create in MyAccount Portal = Two (2) hours</p> <p>Incident Management Resolution Target: Six (6) Hours</p>	Rogers will issue a credit you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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.	<p>Response Target Metric:</p> <p>When you call in live 24x7 = Live answer</p> <p>When you create a MyAccount Portal = Two (2) hours</p> <p>Incident Management Resolution Target: Fourteen (14) Hours</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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.	<p>Response Target Metric:</p> <p>When you call in live 24x7 = Live answer</p> <p>When you create in MyAccount Portal = Two (2) hours</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.

		Incident Management Resolution Target: Seventy-two (72) Hours	
Service Request	Response Time Target as indicated below.	<p>Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours</p> <p>Service Request Resolution Target: Five (5) Business Days (Monday to Friday 8am to 8pm EST)</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.
Move/Add/Change/Delete (MACD) Request	Response Time Target as indicated below.	<p>Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours</p> <p>MACD Request Resolution Target: Scoping performed on a case by case basis</p>	SLO Only (no service credit)

14.2 Incident Management Severity Levels (Table 2):

- 14.2.1 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 your Content is at a significant risk of loss or corruption; you have had a substantial loss of service; and your business operations have been severely disrupted.
- 14.2.2 Severity 2: Major functionality is severely impaired. High impact; and Degradation of critical service or total of loss non-critical services
- 14.2.3 Severity Level 3 (S3) Partial, non-critical loss of functionality of the Services. Low impact – no direct business impact; and Non-critical services affected;
- 14.2.4 Service Request: A request from you 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).
- 14.2.5 Move/Add/Change/Delete (MACD) Request: Are requests which are ‘add-ons’ or compliment the Managed Private Cloud 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.

14.3 Calculation for Response Time and Resolution Target for Incident Management, except if SLO (Table 2):

- 14.3.1 Response Time Target Rogers response time will be measured from the time you call or create 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 you.
- 14.3.2 Rogers’ resolution will be measured from the time you call or create an Incident ticket in MyAccount Portal (Rogers Support System) to the time a Rogers employee updates the Rogers Support System ticket informing you the incident is resolved.

14.4 Monthly Service Level Credit Limitation. 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.

14.5 Service Credit Request Process. If Rogers has failed to meet any of the above service levels for a particular Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.

- 14.6 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Managed Private Cloud Services. You 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 you will be entitled to as outlined within this SLA.

15 Fully Managed Infrastructure & Hypervisor

- 15.1 Fully Managed. With Fully Managed Services, the Private Cloud Services Infrastructure described above and in any Private Cloud Service SOW will be monitored according to manufacturer recommended KPI thresholds. Alerts, reporting and scheduled patching are included with Fully Managed Infrastructure. Rogers will make every reasonable effort to solve an Incident related to the Private Cloud Services Infrastructure, subject to the conditions set out in Section 15.2 below.
- 15.2 Fully Managed Restrictions. Rogers is unable to provide Fully Managed Services for Private Cloud Services in the following circumstances:
- Where the Incident is determined to be caused by a software application issue; or
 - Where the Incident is determined to be caused by inadequate infrastructure.

In any of the above circumstances, Rogers will continue to support you on a reasonable effort's basis. Reasonable efforts support includes two (2) hours of Rogers' onsite support during an Incident. Any effort in excess of two (2) hours will be billable to you at the standard time and materials rate. Rogers will seek written approval from you prior to commencing such billable support.

16 **Your obligations regarding the Microsoft Services Provider License Agreement ("SPLA")**

- 16.1 If you wish to license eligible Microsoft software products to use as part of your Managed Private Cloud Services, you must agree to the Microsoft Services Provider License Agreement ("**SPLA**") terms. The terms and conditions applicable to SPLA are available at <https://www.microsoft.com/en-us/licensing/product-licensing/products>.
- 16.2 You will ensure that you are up to date with all licenses purchased under the SPLA, (the "**Microsoft Licenses**") and will review your Microsoft License usage on a regular basis.
- 16.3 You agree to participate in any Rogers or Microsoft requested audit or any Microsoft License audit requested by Rogers. Any failure on the part of you to comply with such a request and/or participate in such an audit may result in your Services being terminated at Rogers sole discretion.
- 16.4 You further agree:
- a) That Rogers does not control the costs of the Microsoft Licenses;
 - b) That the Microsoft License costs may fluctuate solely at Microsoft's discretion;
 - c) That the Microsoft License usage and the measurement of the usage is at Microsoft's sole discretion;
 - d) To pay any applicable Microsoft License fees when they come due;
 - e) That the price to you represents a committed spend amount and that the price may increase based on your actual Microsoft License usage;
 - f) That Rogers may assess your use of Microsoft Licenses on an annual basis or as otherwise required by Rogers or Microsoft;
 - g) That Rogers may make the needed price adjustments to your invoice for the Microsoft Licenses on an annual basis or as otherwise required, at Rogers' sole discretion;
 - h) That Rogers may make any adjustments to your bill for any unreported Microsoft License usage;
 - i) To review and update your Microsoft license usage no less that four (4) times a year or any time they update or change your usage of the Services in any manner;

- j) That your Microsoft License usage may change due to service requests, incident requests and move/add/change (“**MAC**”) requests made to Rogers and you agree to pay any fees for such changes including Microsoft License fees.

- 17 **License Mobility** – If you make use of Microsoft License mobility – you are responsible for disclosing such use, for all costs associated with the usage, for providing all applicable documentation to Rogers as the Microsoft Licenses are updated. You also agree to ensure that the Microsoft License mobility agreement and any applicable Software Assurance is kept up to date.
- 18 **Virtual machines** - If you import or clone a virtual machine or the image of a virtual machine into the Services, you agree to pay and report for all Microsoft License fee usage resulting from such import or clone.
- 19 **Rogers SPLA Program** – Rogers has three SPLA related programs. Selection of one of these programs is a requirement to receive the Services. The three programs are:
 - 19.1 Outsourced (No SPLA) - you are responsible for all Microsoft licenses on the Service. This is available only where the client has dedicated hardware or where you own the hardware.
 - 19.2 OS-Only - Rogers is responsible for the Microsoft OS license. All other Microsoft services licenses are the responsibility of you and need to have Service Assurance with authorization for License Mobility to deploy on the services.
 - 19.3 SPLA - Rogers is responsible for the Microsoft OS licenses and SQL licenses up to Standard only. All other Microsoft services licenses are the responsibility of you and need to have Service Assurance with authorization for License Mobility to deploy on the services.
 - 19.4 If you do not select a program, the default program will be Outsourced.

20 **Termination Fees**

- 20.1 If you terminate the Managed Private Cloud Services without cause, or if Rogers terminates the Managed Private Cloud Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:
 - a) One hundred (100%) 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;
 - b) One hundred percent (100%) of the unpaid charges for the terminated Service(s); and
 - c) One hundred percent (100%) of any outstanding usage and/or overage charges.
- 20.2 Where you terminate the Managed Private Cloud Services prior to the expiration of the Initial Service Term or Renewal Service Term, as applicable, you shall either return all Rogers Equipment associated with the Managed Private Cloud Services to Rogers or pay to Rogers the fair market value of such Rogers Equipment.

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

Business Resumption

The following terms pertain specifically to Business Resumption supplied by Rogers to you.

1. Features

Business Resumption Services from Rogers ("**Services**") are available in combination with Rogers hosted, virtual and colocation Services, which are each described in a separate Colocation Services Schedule. Business Resumption Services have the following features:

- 1.1 Workstation electrical power in the Dedicated Business Resumption Facility (DBRF) will be connected to Rogers' diesel power generator.
- 1.2 Access to your Dedicated Business Resumption Facility is on a 7x24x365 basis.
- 1.3 Unless otherwise set forth in the Agreement, all power in the Dedicated Business Resumption Facility is based on existing building electrical services.
- 1.4 Use of common areas, including washrooms, is available, as determined by Rogers.

The following optional features can be purchased by you in combination with Business Resumption Services for an additional charge, to be quoted by Rogers upon request:

- 1.5 Direct fibre connectivity from servers in the Data Center to the Dedicated Business Resumption Facility.
- 1.6 Additional electrical outlets and Ethernet jacks.
- 1.7 Access to telecommunications technical (connectivity) equipment and services provider.

2. Definitions:

- 2.1 Acceptable Downtime means any of the following events: Scheduled Maintenance; Emergency Maintenance; your breach of the Agreement; order suspensions due to your credit worthiness; failure of your applications or your equipment not within the sole control of Rogers or its subcontractors; any act or omission by you or user of the Business Resumption Services authorized by you; any event of Force Majeure.
- 2.2 Data Centre (or Colocated Site) means the physical Rogers data centre location in which the Services are made available to you by Rogers, as specified in the attached Agreement (s).
- 2.3 Dedicated Business Resumption Facility or DBRF Dedicated Business Resumption Facility means the portion(s) of the Data Centre made available to you for the Services, plus any other space that is required to provide the Services.
- 2.4 Emergency Maintenance means any urgent maintenance activities performed on the Rogers' infrastructure connected to your equipment in order to prevent or address imminent failures affecting Rogers' infrastructure.
- 2.5 Incident. Incident means an unplanned interruption to a Service or reduction in the quality of a Service that you have enrolled for Business Resumption.
- 2.6 Monthly Recurring Charge – means the monthly charge for each Service.
- 2.7 Qualified Outage means a service-impacting loss of service elements for at least 10 consecutive minutes (only one Qualified Outage per day allowed).

- 2.8 Scheduled Maintenance. Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected provided that you shall be given at least forty-eight (48) hours' advance notice of such maintenance activities. Such activities are typically performed during the standard maintenance window on Tuesdays, Thursdays and Sundays from 12AM to 7AM Eastern Time.

3. Term, Rates, and Charges

- 3.1 The term of each Business Resumption Service (each an “**Initial Service Term**”) is as set forth in the Agreement (s). The term of this Schedule commences on the date of signature of the Agreement by you, or, if this Schedule is attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon expiration of the Initial Service Term, a Business Resumption Service may be renewed for an additional period set forth in an Agreement to be added to this Agreement by way of amendment (a “**Renewal Service Term**”) or, if no amendment is executed, the Business Resumption 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**”.
- 3.2 The Fees for the Business Resumption Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement (s). Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Business Resumption Services by any third party or unauthorized person.
- 3.3 Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Monthly Recurring Charges set out in any applicable Agreement represent minimum charges. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 3.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Business Resumption Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Business Resumption Services or thirty (30) days after 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 your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 3.5 Rogers reserves the right to change rates for any and all Business Resumption Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.
- 3.6 Upon the commencement of a Month-to-Month Renewal Term for a Business Resumption Service, the rates for such Business Resumption Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 3.7 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

4. Services, Equipment, and Maintenance

- 4.1 All interest in and ownership of your Equipment and the content on such your Equipment including, but not limited to, those portions of the content that are your trade names, trademarks or service marks, are and shall remain the property of you, or the registered owner of such your Equipment or content, as applicable.
- 4.2 You or your agents are responsible for maintaining the applications, operating systems and hardware equipment.

- 4.3 In order to continue reliable Services operation Rogers requires that periodic routine scheduled maintenance be performed on all Services support infrastructure, including, without limitation, electrical and mechanical. Most of the maintenance services are performed without any impact on the Services operation or interruption to the Services.
- 4.4 On an annual basis Rogers may require maintenance services to be performed on the major power distribution systems to the DBRF. This action will necessitate the total removal of power from the DBRF. At this time there may be a requirement for you to shut down your equipment for this service to be completed. A minimum of one (1) month advance notice will be given to you that may be affected by this interruption. If a total shutdown of your hardware is not possible then Rogers is willing to provide alternative power options at a cost to you.
- 4.5 You grant Rogers' permission to perform routine and scheduled maintenance on all DBRF electrical and mechanical support equipment that may be located in your caged area or suites.

Routine scheduled maintenance performed on service level elements (Non-intrusive preventive maintenance)	Performed Monthly
Advance notice of routine scheduled maintenance on service level elements (possible service interruption)	Minimum one (1) month notice
Non-scheduled emergency maintenance	Communicated immediately to you

5. **Security Access and Fraud**

- 5.1 You are solely responsible for any non-physical security breach or unauthorized usage of the Business Resumption Services, your equipment, including unmanaged Rogers' equipment, and your accounts.
- 5.2 Rogers will take precautions and use commercially reasonable efforts to secure Rogers Equipment, excluding unmanaged Equipment provided by Rogers, and Rogers Service platforms and, as determined by Rogers, to identify security breaches. Notwithstanding any action of Rogers, you are solely responsible for security of your data. Where a situation is considered a security breach, Rogers shall notify you as soon as commercially reasonable and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 5.3 You are solely responsible for establishing access and user management controls that clearly identify individuals who have access to your account administration, security, technical and/or billing rights ("**Access Control and User Management Controls**") and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to you Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential.
- 5.4 You access to your equipment and the DBRF is through the use of a proximity card reader. All proximity card accesses are logged, and reports of your accesses is available via the online customer portal. Video surveillance cameras are located at each door entrance / exit to monitor traffic. The video feed is digitally recorded for later review if necessary (30 day retention).
- 5.5 Rogers will track all access to your system through an online ticketing system and ensure that those who requested access have all necessary documented your approvals prior to accessing your environment.
- 5.6 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Business Resumption Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.

- 5.7 In the event of any emergency that presents a risk of an Out of Service Condition, or damage to you or Rogers' Equipment or data belonging to Rogers, a third party, Rogers' facilities, or to any persons or property present therein, Rogers will take all measures it deems reasonable to respond to the emergency or threat. Rogers, acting reasonably, may disable Services and Rogers Equipment, (and disable or remove your Equipment, if necessary) to address the emergency or immediate threat. Rogers shall use commercially reasonable efforts to notify you prior to disabling or removing your equipment, and in any case will notify you thereafter.

6. Site Access

- 6.1 You shall not seek to or acquire any rights or interest in the Colocated Site, the Rogers' Equipment or any portion of the Colocated Site as a result of the Agreement or its termination for any reason.
- 6.2 Rogers shall provide reasonable commercial physical access to the Colocated Site to your authorized individuals identified through your Access Control and User Management Controls ("**Authorized Individuals**"), subject to the terms and conditions of this Schedule, and may require that a Rogers authorized employee accompany your Authorized Individuals. In such a case where you requires that a Rogers authorized employee accompany Authorized Individual(s), then you shall give a minimum of four (4) hours advance notice to Rogers' Corporate Support team (the technical support group at Rogers responsible for handling support requests from you for the Business Resumption Services) for access to any Colocated Site, unless otherwise indicated by Rogers, provided that in case of an emergency, such access may be delayed and Rogers shall provide a reasonable estimate of the duration of such delay. You shall be fully responsible for the acts and/or omissions of Authorized Individuals or agents inside the Colocated Site.
- 6.3 All visitors must present a valid government issued photo ID and be authorized in advance by you, subject to Rogers' approval, to access the Rogers environment. If Rogers' records indicate that a visitor is not designated as a Authorized Individual, the visitor will not be granted access to the Colocated Site.
- 6.4 All emergencies and suspicious behaviour noted at the Colocated Site by you must be immediately reported to the Rogers security desk.
- 6.5 Rogers reserves the right to inspect your environment upon the provision of reasonable advance notice and with you, or an Authorized Individual, present.

7. Product Service Level Agreement ("SLA")

- 7.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("**Service Credit**").

Table 1: Power Availability

	Power Availability	Service Level Credit
Uptime to power that feeds the Colocated Site (excluding the following: unplanned window of up to 8 hours to facilitate any upgrades and periodic maintenance that may be required to ensure a safe and reliable power source, Scheduled Maintenance, and Acceptable Downtime)	99.9% or less than 43 minutes of unscheduled downtime	One (1) of pro-rated day credit of recurring charges per Qualified Outage (maximum one per day)

- 7.2 The following conditions will apply before any credit is calculated:

- 7.2.1 If information or input is required from you to resolve a situation then the trouble will be deferred until such time that the appropriate information is received from you. Deferral stops escalation and outage calculation against the SLA
- 7.2.2 You are responsible for reporting outages;
- 7.2.3 Time calculation will start only after the notification is received by Rogers from you
- 7.2.4 Outages must ten (10) or more minutes in length
- 7.2.5 Rogers' SLAs do not include connectivity services provided by third party network providers, even where Rogers coordinates billing administration. Connectivity issues with third party services should be directed to the appropriate service provider and are not the responsibility of Rogers.
- 7.3 Outage Notification. You shall notify Rogers of any outage by opening a trouble ticket with Rogers Customer Care within one (1) day for any Power Availability, following which Rogers shall validate the outage. If Rogers determines that there is an outage, Rogers will record it as an Out-of-Service condition in its system.
- 7.4 Monthly Service Level Credit Limitation. The combined cumulative total of all Service Credits for a calendar month for the Business Resumption Services will not exceed the total Monthly Recurring Charges for the affected Business Resumption Sites that Rogers has invoiced for such calendar month.
- 7.5 Service Credit Request Process. If Rogers has failed to meet any of the above service levels for a particular Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.
- 7.6 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Business Resumption Services. You 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 you will be entitled to as outlined within this SLA.

8. Termination Fees

- 8.1 If you terminate the Business Resumption Services without cause, or if Rogers terminates the Business Resumption Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:
 - 8.1.1 fifty (50%) percent of the average monthly charges per terminated Business Resumption 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;
 - 8.1.2 any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the applicable Business Resumption Service that exceeds the amount set out in (a) above; and
 - 8.1.3 a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Business Resumption Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Business Resumption Service.

- 8.2 Where you terminate the Business Resumption Services prior to the expiration of the Initial Service Term or Renewal Service Term, as applicable, you shall either return all Rogers Equipment associated with the Business Resumption Services to Rogers or pay to Rogers the fair market value of such Rogers Equipment.
- 8.3 The above shall be included in an invoice to your subsequent to termination.

Managed Services

The following terms pertain specifically to Managed Services supplied by Rogers to you.

1. **Definitions.** Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:
 - 1.1 Acceptable Downtime. means any of the following events: Scheduled Maintenance; Emergency Maintenance; your breach of the Agreement; order suspensions due to your credit worthiness; failure of your applications or your equipment not within the sole control of Rogers or its subcontractors; any act or omission by you or user of the Managed Services authorized by you; any event of Force Majeure.
 - 1.2 Colocated Site means the physical Rogers data centre location in which Space for your equipment is made available by Rogers, as specified in the attached Agreement(s).
 - 1.3 Corporate Support Team. Corporate Support Team means the technical support group at Rogers responsible for handling all support requests from the you for the Services.
 - 1.4 Emergency Maintenance means any urgent maintenance activities performed on the Rogers' infrastructure connected to Space or your equipment in order to prevent or address imminent failures affecting Rogers' infrastructure.
 - 1.5 End-user. End-user means any person enabled, through a data connection over the internet, to access, use, purchase, download, or otherwise interact with your content, which is located on or distributed by means of your Equipment.
 - 1.6 Incident. Incident means an unplanned interruption to a Service or reduction in the quality of a Service that you have enrolled for Managed Network Services.
 - 1.7 Mean Time to Repair (MTTR). MTTR means the average length of time it took to repair or resolve an Incident during a specific month, excluding Acceptable Downtime. MTTR metrics are based solely on the Incident Repair Time statistics collected by the Rogers Trouble Reporting System (TRS). MTTR is calculated with the following formula: Mean Time to Repair = Incident Repair Time in one month (hours) ÷ Number of Incidents in same month.
 - 1.8 Out of Service Condition means a condition whereby there is a Managed Service outage, excluding any Managed Service outage resulting from an Acceptable Downtime.
 - 1.9 Scheduled Maintenance. Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected provided that you shall be given at least forty-eight (48) hours' advance notice of such maintenance activities. Such activities are typically performed during the standard maintenance window on Tuesdays, Thursdays and Sundays from 12AM to 7AM Eastern Time.
 - 1.1 Space means a designated section of the Colocated Site where space of one or more equipment cabinets (or racks) are set-aside by Rogers for your equipment.
2. **Features.** Rogers' Managed Services are available either as Managed Network Services or Managed Server Administration Services (collectively "**Managed Services**" or "**Services**", as applicable), in the types detailed below:

2.1 Managed Network Services:

- 2.1.1 Managed Router. Managed Router Services involve Rogers managing your router on its behalf. You do not have access to the router. Managed Router Services include:
 - real-time SNMP monitoring;
 - daily back-ups of the router configuration for rapid restoration of the hardware;
 - real-time logging of all router devices to a Rogers log server;
 - reporting of router interface traffic in 5 minute intervals and graphing of results in your portal;
 - reporting of interface errors in 60 minute intervals and graphing of results in your portal;
 - reporting of CPU and memory usage in 5 minute intervals and graphing in your portal;
 - performance of router configuration changes as requested by you (2 configuration changes are included per month, after which there is a one-time charge per change, which is currently \$50.00, but is subject to change without notification);
 - OS patching and hotfix;
 - monitoring of all up-links for up/down status and incident management as required; and
 - monitoring of bandwidth thresholds and incident management as required.

- 2.1.2 Managed Switch. Managed Switch Services involve Rogers managing your switch on your behalf. You do not have access to the switch. Managed Switch Services include:
- a) real-time SNMP monitoring;
 - b) daily back-ups of the switch configuration for rapid restoration of the hardware;
 - c) real-time logging of all switch devices to a Rogers log server;
 - d) reporting of switch interface traffic in 5 minute intervals and graphing of results in your portal;
 - e) reporting of interface errors in 60 minute intervals and graphing of results in your portal;
 - f) reporting of CPU and memory usage in 5 minute intervals and graphing in your portal;
 - g) performance of switch configuration changes as requested by you (2 configuration changes are included per month, after which there is a one-time charge per change, which is currently \$50.00, but is subject to change without notification);
 - h) OS patching and hotfix;
 - i) monitoring of all up-links for up/down status and incident management as required; and
 - j) monitoring of bandwidth thresholds and incident management as required.
- 2.1.3 OfficeLink Secure. OfficeLink Secure Services include rental of a firewall device (Cisco ASA or Fortinet) and Rogers' management of that device, as well as VPN management (site to site, and remote). OfficeLink Secure Services include:
- a) a turn-key managed WAN-facing, VPN concentrator site location solution;
 - b) 24 x 7 firewall monitoring which includes availability, concurrent connections, memory usage, device health, and SNMP MIBII variables;
 - c) 24 x 7 firewall Access Control List (ACL) with logging to a syslog server;
 - d) access to online maintenance and incident response service via your portal;
 - e) firewall software maintenance and updates, as released by the firewall manufacturer;
 - f) 2 firewall rule changes per month, to a maximum of 30 minutes each, after which hourly charges apply;
 - g) up to 3 Internal/VLANs configured;
 - h) up to five (5) IPSec VPN tunnels with 168-bit triple DES VPN encryption; and
 - i) hardware replacement Next Business Day (NBD), except for rural areas which is subject to availability of delivery.
- 2.1.4 Managed Firewall. Managed Firewall Services include management of Cisco ASA or Fortinet devices. You supply the device. You must have a Cisco Smartnet warranty on any managed Cisco device and Fortinet support and on Fortinet device. Managed Firewall Services include:
- a) management of your existing Cisco ASA or Fortinet firewall;
 - b) 24 x 7 monitoring of availability, concurrent connections, memory usage, device health, and SNMP MIBII variables;
 - c) logging and reporting include 24 x 7 firewall Access Control List (ACL) logging to a syslog server
 - d) access to online maintenance and incident response service via your portal;
 - e) firewall software maintenance and updates, as released by the firewall manufacturer;
 - f) 2 firewall rule changes per month, to a maximum of 30 minutes each, after which there is an hourly charge, to be quoted by Rogers.
- 2.1.4.1 Managed Firewall Add-on Features. The following features are available as optional add-ons:
- a) management of Fortinet Unified Threat Management (UTM) solution;
 - b) enhanced reporting available via FortiAnalyzer (additional monthly fees apply).
- 2.1.5 Managed Firewall Service - Cloud UTM Managed Firewall Services for Public Cloud include management of the Sophos UTM v9 virtual firewall appliance. The virtual device is supplied by Rogers as part of the Public Cloud Services. Managed Firewall Services for Public Cloud include:
- a) management of a Sophos UTM v9 virtual firewall;
 - b) 24 x 7 monitoring of availability, concurrent connections, memory usage, device health, and SNMP MIBII variables;
 - c) logging and reporting include 24 x 7 firewall Access Control List (ACL) logging to a syslog server;
 - d) access to online maintenance and incident response service via your portal;

- e) firewall software maintenance and updates, as released by the firewall manufacturer;
- f) two (2) firewall rule changes per month, to a maximum of 30 minutes each, after which there is an hourly charge, to be quoted by Rogers.

2.2 Managed Server Administration Services:

- 2.2.1 Managed Server Administration Tiers. Managed Server Administration Services are offered in three tiers: Self-Serve Monitoring and Alerting, Proactive Monitoring, Patching and Reporting, and Fully Managed.
- 2.2.2 Self-Serve Monitoring and Alerting. This tier of Managed Server Administration Services provides key your server component monitoring, threshold alerts and reporting, with extra support available on a pay-per-use basis.
- 2.2.3 Proactive Monitoring, Patching and Reporting. This tier of Managed Server Administration Services includes the same features as the Self-Serve Monitoring and Alerting tier, plus scheduled OS patching.
- 2.2.4 Fully Managed. This tier of Managed Server Administration includes the same features as the Proactive Monitoring, Patching and Reporting tier, plus onsite support as required at no additional cost. The Fully Managed tier of Managed Server Administration includes Rogers' support of you to make every reasonable effort to solve any Incident. Certain conditions apply, as set out below.

2. Term, Rates, and Charges

- 2.1 The term of each Managed Service (each an “**Initial Service Term**”) is as set forth in the Agreement(s). The term of this Schedule commences on the date of signature of the Agreement by you, or, if this Schedule is attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon expiration of the Initial Service Term, Managed Services may be renewed for an additional period set forth in an Agreement to be added to this Agreement by way of amendment (a “**Renewal Service Term**”) or, if no amendment is executed, the Services 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**”.
- 2.2 The Fees for the Managed Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Professional Service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Managed Services by any third party or unauthorized person. In the case of Managed Firewall Services for Public Cloud (as part of the Managed Network Services), you are responsible for all monthly and hourly Public Cloud Services charges in relation to the delivery of the Managed Firewall Services. This includes, but is not limited to, virtual machines, V-racks, IPs, storage, and bandwidth. Unless otherwise specified in the Agreement, there are no limits or restrictions on usage.
- 2.3 Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 2.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Managed Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Managed Services 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 your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 2.5 Rogers reserves the right to change rates for any and all Managed Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.
- 2.6 Upon the commencement of a Month-to-Month Renewal Term for Managed Services, the rates for such Services will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 2.7 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

3. Services and Equipment.

- 3.1 Remote Hands. Rogers will make available personnel (“**Remote Hands**”) who will, upon your request and availability, provide non-technical support and assistance. Rogers will respond to a reasonable number of requests based on the size of the installation, and response times will be based on a best-efforts basis. Remote Hands will act only upon request and direction from you. Rogers is not responsible or liable for any consequences of the actions performed upon your request by Remote Hands.
- 3.2 Ownership in your Equipment and Content. All interest in and ownership of your Equipment and the content on your Equipment including, but not limited to, those portions of the content that are your trade names, trademarks or service marks, are and shall remain the property of you, or the registered owner of your Equipment or content, as applicable.
- 3.3 Your Equipment Ownership Requirements. Where you have purchased Managed Firewall Services (Managed Network Services) or Fully Managed Server Administration (Managed Server Administration Services), the equipment under management may be owned by Rogers or by you. If the equipment is owned by you, the following conditions must be in place in order for Rogers to perform the appropriate Managed Services:
- a) Your Equipment must have an up-to-date warranty or equipment maintenance contract valid for the entirety of the Service Term for appropriate Managed Services;
 - b) Your Equipment must have a supported OS with up-to-date patching; and
 - c) You must provide Rogers with physical and remote access to your Equipment.
- 4.4 Managed Services Restrictions. Rogers is unable to provide Managed Firewall Services (Managed Network Services) or Fully Managed Server Administration (Managed Server Administration Services) in the following circumstances:
- a) Where the equipment vendor deems the equipment unrepairable;
 - b) Where a disaster situation renders the equipment inoperable, unrepairable or unreachable;
 - c) Where the Incident is determined to be caused by a software application issue;
 - d) Where the Incident is determined to be caused by inadequate infrastructure;
 - e) Where you elect to opt out of Scheduled Maintenance for a period longer than six (6) consecutive months; and
 - f) Where your Equipment does not meet the conditions described in Section 4.3 above.

In any of the above circumstances, Rogers will continue to support you on a best effort basis. Best efforts support includes two (2) hours of Rogers’ onsite support during an Incident. Any effort in excess of two (2) hours will be billable to you at the standard pay-per-use rate. Rogers will seek written approval from you prior to commencing such billable support.

4. Security Access and Fraud

- 4.1 Rogers shall use commercially reasonable efforts to secure Rogers Equipment, excluding unmanaged Equipment provided by Rogers, and Rogers Service platforms. Notwithstanding any action of Rogers, you are solely responsible for security of your data. Where a situation is considered a security breach, Rogers shall notify you as soon as feasible and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 4.2 You are solely responsible for establishing access and user management controls that clearly identify individuals who have access to your Space, account administration, security, technical and/or billing rights (“**Access Control and User Management Controls**”) and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to your Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize

strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential.

- 4.3 Rogers will track all access to your Managed Services through an online ticketing system and ensure that those who requested access have all your necessary documented approvals prior to accessing your Managed Services.
- 4.4 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Managed Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.
- 4.5 In the event of any emergency that presents a risk of an Out of Service Condition, or damage to you or Rogers' equipment or data belonging to Rogers, a third party, the Colocated Site, or to any persons or property present therein, Rogers may rearrange your equipment as is reasonably necessary to respond to the emergency. Additionally, and only as necessary, Rogers may disconnect or remove your equipment if the emergency requires such disconnection or removal to avoid damage. Rogers shall use commercially reasonable efforts to notify you prior to rearranging, disconnecting or removing your equipment, and in any case will notify you thereafter.

5. **Product Service Level Agreement ("SLA")**

- 6.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("Service Credit").

Table 1: Managed Services Incident Reporting

Service	Incident Reporting	Service Level Credit
Proactive Monitoring or Fully Managed tier of the Managed Server Administration Services; or Managed Router, Managed Switch, Managed Firewall or OfficeLink Secure type of Managed Network Services	Notify you within thirty (30) minutes after Rogers determines that your component on which Managed Services is provided has experienced an issue, excluding Acceptable Downtime. The particular Managed Service tier purchased will dictate the method of reporting.	Upon your written request and Rogers' confirmation that the Managed Services Incident Reporting SLA was not met, your account shall be credited for one (1) day of pro-rated monthly recurring charges for the Managed Services for each instance the Managed Services Incident Reporting SLA was not met for reasons other than Acceptable Downtime, provided that only one such Managed Services Incident Reporting Service Credit can be applied for any one calendar day, despite the number of Managed Services Incident Reports missed on that calendar day.

- 6.2 Incident Validation and Reporting Process (Table 1). You must complete a Customer Information Form in its entirety and submit such form to Rogers at myaccount.datacentres.rogers.com. You are solely responsible for providing Rogers accurate and current contact information for your designated points of contact. Rogers will be relieved of its obligations under the Managed Services Incident Reporting SLA if your contact information is out of date or inaccurate due to your action or omission.

TABLE 2: Mean Time to Repair (MTTR) Commitment

Service	Monthly MTTR	Service Credit
Managed Router or Managed Switch of Managed Network Services; or Fully Managed tier of Managed Server Administration Services	< 8 h	The MTTR commitment specifically pertains to the interval between when an Incident has been identified and when Rogers has either notified you that the Incident has been resolved or has proposed a workaround to the Incident to you, excluding Acceptable Downtime and Managed Services Restrictions as described in Section 4.4 above. Upon Rogers' verification that the MTTR over a given billing month was longer than the MTTR commitment, Rogers will issue a Service Credit to you representing 50% of the monthly recurring charges for the Managed Services.

- 6.3 MTTR Validation and Reporting Process (Table 2). You must request each month's measurements from your Rogers sales representative by the fifteenth (15th) day of the following month. Rogers Trouble Reporting System (TRS) data will be used to determine MTTR metrics and your eligibility for a Service Credit.
- 6.4 The combined cumulative total of all Service Credits for a calendar month for the Managed Services will not exceed the total Monthly Recurring Charges for the affected Managed Services Sites that Rogers has invoiced for such calendar month.
- 6.5 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Managed Services. You 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 you will be entitled to as outlined within this SLA.

7 Termination Fees.

- 7.1 If you terminate the Services without cause, or if Rogers terminates the Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:
- a) One hundred (100%) 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 of 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;
 - b) any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the applicable Service that exceeds the amount set out in (a) above; and
 - c) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Service.
- 7.2 Where you terminate the Managed Services prior to the expiration of the Initial Service Term or Renewal Service Term, as applicable, you shall either return all Rogers Equipment associated with the Managed Services to Rogers or pay to Rogers the fair market value of such Rogers Equipment.
- 7.3 The above shall be included in an invoice to your subsequent to termination.

Managed Cloud Backup Services (HFX)

The following terms pertain specifically to Managed Cloud Backup Services (HFX) supplied by Rogers to you.

Managed Cloud Backup Services (“**Services**” or “**Service**”) are available to you if you have purchased Rogers Cloud Backup Services at an eligible Rogers data centre or if you have purchased Rogers Private Cloud Services or Rogers Public Cloud Services.

1. Features. Managed Cloud Backup Services include the following core and optional features:

- 1.1 Cloud Backup Storage. Cloud Backup includes an initial full backup of your data to one of Rogers’ owned data centres. From that point on incremental backups are taken. Each day an incremental backup is taken. On day 7, the 6 daily backups are rolled up into a synthetic weekly full backup. At the end of 4 weeks the 4 weekly backups are rolled up into a monthly backup. Your data is kept for a pre-determined retention period and Rogers will begin to restore it to you when you log a Live Answer request with Rogers Corporate Support Team during that retention period.
- 2.1 Cloud Backup with Geodiversity. Where requested by you and for an additional charge as set out in the Quotation, the Cloud Backup Services are available with geodiversity, which refers to a second backup copy of your data that is transmitted and stored daily to a second Cloud Backup location in a second city.
- 3.1 Cloud Backup Data Retention. Managed Cloud Backup Services are available in one standardized retention period: 14 days. At the end of the retention period your data “ages out” and is no longer available to you for restoration.
- 4.1 Cloud Backup Supported Applications. Managed Cloud Backup Services can be used to backup data from a wide range of applications, including: Windows File System; Linux File Systems; Active Directory; Databases such as MS SQL, MySQL, PostgreSQL, Oracle, Lotus Notes Database, and SAP; MS Exchange (server and mailboxes); MS Sharepoint; and Lotus Notes Documents. You are encouraged to contact your Rogers’ representative to determine if your specific application(s) can be backed up using Managed Cloud Backup Services.
- 5.1 Cloud Backup Encryption Options. A unique encryption key is generated by the Rogers Cloud Backup platform for each backup and is required in order for restored data to be readable.
- 6.1 Cloud Backup Restoral Options. When restoral of your data is requested and confirmed, your data on physical machines (ie. that is stored on Colocated Services) is restored at the file level. Your data on virtual machines can be restored as an image (ie, a snapshot like backup is taken) or at a file level, based on your preference that was established at time of initial Cloud Backup implementation.
- 7.1 Cloud Backup Reporting. You will receive a daily email outlining the quantity of Cloud Backup data per your system. Historical data reporting is available on the myAccount portal.
- 8.1 Cloud Backup Customer Portal. An enhanced customer portal is made available to Cloud Backup customers. This portal will provide:
 - improved reporting, including logs, usage and metadata;
 - the ability for you to initiate your own data backup;
 - the ability for you to initiate your own data restore.

2. Definitions. Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:

- 2.1 Acceptable Downtime. means any of the following events: Scheduled Maintenance; Emergency Maintenance; your breach of the Agreement; order suspensions due to your credit worthiness; failure of your applications or your equipment not within the sole control of Rogers or its subcontractors; any act or omission of you or user of the Colocation Services authorized by you; any event of Force Majeure.

- 2.2 Business Day. Monday to Friday inclusive, excluding statutory holidays observed in the Province of Nova Scotia.
- 2.3 Cloud Backup Availability. Cloud Backup Availability means the percentage of time during a specific calendar month that the Services are available for your use, as set out in this Schedule. Cloud Backup Availability is based on ticket information from Rogers Customer Care. If an Out of Service condition is detected or reported, the Cloud Backup Services will be deemed to be unavailable for the length of the Out of Service condition. Cloud Backup Availability is calculated as the total number of minutes that the Services were unavailable during a specific month, divided by the total number of minutes in the specific month, multiplied by hundred (100) (for the percentage).
- 2.4 Emergency Maintenance means any urgent maintenance activities performed on the Rogers' infrastructure connected to Space or your equipment in order to prevent or address imminent failures affecting Rogers' infrastructure.
- 2.5 Colocated Site means the physical Rogers data centre location in which Space for your equipment is made available by Rogers, as specified in the attached Quotation(s).
- 2.6 Corporate Support Team. Corporate Support Team means the technical support group at Rogers' responsible for handling all support requests from you for the Services.
- 2.7 Out of Service Condition means a condition whereby there is a Service outage, excluding any Service outage resulting from an Acceptable Downtime.
- 2.8 Power Availability. Power Availability means the percentage of time during a specific calendar month that the power supply to your particular Space is available. For redundant power configuration, failure of both A and B PDU circuit(s) at the same time will be considered an Out of Service condition for Power Availability. Power Availability is based on ticket information from Rogers Customer Care. If an Out of Service condition is detected or reported on a specific power supply, the power supply will be deemed to be unavailable for the length of the Out of Service condition. Power Availability is calculated as the total number of minutes that the power supply was unavailable during a specific month, divided by the total number of minutes in the specific month, multiplied by hundred (100) (for the percentage).
- 2.9 Recovery Point. Recovery Point refers to the timestamp and quantity of your data available to restore. Your data is backed up nightly, therefore you have one (1) Recovery Point per day.
- 2.10 Scheduled Maintenance. Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected provided that you shall be given at least forty-eight (48) hours' advance notice of such maintenance activities. Such activities are typically performed during the standard maintenance window on Sundays from 1AM to 7AM local Time.
- 2.11 Space means a designated section of the Colocated Site where space of one or more equipment cabinets (or racks) are set-aside by Rogers for your equipment.

3. Term, Rates, and Charges

- 3.1 The term of this Schedule commences on the date of signature of the Agreement by you, or inclusion of this Schedule to the Agreement by way of amendment and ends on the expiration of the last in force Service Term. The term of each Service (each an **"Initial Service Term"**) is as set forth in the Quotation(s). Upon expiration of the Initial Service Term, a Service may be renewed for the additional period set forth in the Quotation to be added to this Agreement by way of amendment (a **"Renewal Service Term"**) or, if no amendment is executed, the 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"**.
- 3.2 The Fees for the Services, including the Monthly Recurring Charges are set out in the Quotation(s). Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Managed Cloud Backup Services by any third party or unauthorized person.

- 3.3 Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Such charges will commence as of the Service Effective Date. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 3.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Services or thirty (30) days after the Services are made available to you by Rogers in accordance with this Schedule. In the first month, the charges will be prorated for the number of days in the month after the Service Effective Date. Rogers will, by way of invoice or otherwise, notify you of the Service Effective Date. Applicable Service Credits will be applied to your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 3.5 Consumption of Managed Cloud Backup Services is based on the total front end storage to be protected by the Service. Your purchases a quota of front end virtual machine storage to be backed up. You will be charged overage fees if your back end usage exceeds the expected fair use level for the default retention.
- 3.6 Monthly Recurring Charges set out in any applicable Quotation represent minimum charges. You are responsible for all charges for excess usage beyond the minimum Monthly Recurring Charges billed at a twenty-five (25%) percent premium above the monthly rate. Unless otherwise specified, there are no limits or restrictions on usage
- 3.7 Rogers reserves the right to change rates for any and all Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.
- 3.8 Upon the commencement of a Month-to-Month Renewal Term for a Service, the rates for such Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 3.9 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

4. Site Access.

Ownership of Facilities. You will in no case be permitted to access the physical space or the surrounding facility from which the Services are performed. You will not acquire any interest in, nor file any liens upon the Rogers Equipment, or any portion of the data centre as a result of the provision by Rogers of the Services or their termination for any reason pursuant to the Agreement.

5. Security Access and Fraud.

- 5.1. You agree to implement and is solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Services, your equipment, including unmanaged Rogers' equipment, and your accounts.
- 5.2. Rogers shall limit physical access to the Site and use commercially reasonable efforts to prevent unauthorized access to your equipment and, as determined by Rogers, to identify security breaches. Where a situation is considered a security breach, Rogers shall notify you as soon as feasible and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 5.3. You are solely responsible for establishing access and user management controls that clearly identify individuals who have access to your Space, account administration, security, technical and/or billing rights ("**Access Control and User Management Controls**") and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as

well as those authorized to perform any changes to your Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential.

- 5.4. Rogers will track all access to your Services through an online ticketing system and ensure that those who requested access have all necessary documented your approvals prior to accessing your Services.
- 5.5. You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.
- 5.6. In the event of any emergency that presents a risk of an Out of Service Condition, or damage to you equipment or data belonging to Rogers, a third party, the Colocated Site, or to any persons or property present therein, Rogers may rearrange your equipment as is reasonably necessary to respond to the emergency. Additionally, and only as necessary, Rogers may disconnect or remove your equipment if the emergency requires such disconnection or removal to avoid damage. Rogers shall use commercially reasonable efforts to notify you prior to rearranging, disconnecting or removing your equipment, and in any case will notify you thereafter.
- 5.7. You are not permitted to run security penetration tests on the Services without written approval from Rogers and any such actions will be considered improper use under the Agreement. Rogers may, without liability, restrict Services platform access if you perform invasive platform testing without prior written approval.

6. Data Privacy

Except as otherwise set out in the Agreement regarding Rogers' right to access your information, only authorized your personnel can access your data in a readable form while it is housed on the Cloud Backup platform. Rogers' personnel will perform administrative activities on the Cloud Backup platform but will not have access to readable your data. Your data will be retained in Canada, at one of Rogers' secure data centre locations.

7. Encryption

Even where your data is encrypted, if Rogers is under legal obligation to disclose certain information or yours as described in the Agreement, Rogers is obligated to make the encryption keys available along with such lawfully requested data.

8. Service Level Agreement ("SLA")

- 8.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("**Service Credit**").

Table 1: Cloud Backup Availability

	Power Availability	Service Level Credit
Geodiverse Cloud Backup Configuration	100%	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services.
Non-Geodiverse Cloud Backup Configuration	99.95%	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services.

Table 2: Response Time

	Response Time	Service Level Credit (if Response Time not met)
Telephone to Rogers Corporate Support Team	Immediate (ie. LiveAnswer)	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Cloud Backup Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services.
Ticket created in the MyAccount portal	2 hours	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services.
Email sent to Rogers Corporate Support Team	4 hours	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative sixty (60) minutes or fraction thereof, of Response Time in excess of the SLA set out in Table 1 above on a per Incident basis, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services for all Incidents in a particular month.

Table 3: Cloud Backup Recovery Point

	Recovery Point	Service Level Credit
Recovery Point	At least once per forty-eight (48) hours	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative twenty-four (24) hours or fraction thereof, of Recovery Point in excess of the SLA set out above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services for all Incidents in a particular month

8.2 **Outage Notification.** You shall notify Rogers of any outage by opening a trouble ticket with Rogers within five (5) days for any Cloud Backup Availability issue of any Out of Service condition or Response Time misses and one (1) Business Day of any failure to meet the Recovery Point SLA, following which Rogers shall validate the outage. If Rogers determines that there is an outage, Rogers will record it as an Out-of-Service condition in its system.

8.3 **Monthly Service Level Credit Limitation.** 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 Cloud Backup Sites that Rogers has invoiced for such calendar month.

8.4 **Service Credit Request Process.** If Rogers has failed to meet any of the above service levels for a particular Customer Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.

8.5 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Services. You 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 you will be entitled to as outlined within this SLA.

9. Termination Fees

9.1 If you terminate the Services without cause, or if Rogers terminates the Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

- a) 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;
- b) any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the applicable Service that exceeds the amount set out in (a) above; and
- c) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Service.

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

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

Object Store

The following terms pertain specifically to Object Store supplied by Rogers to you.

1. **Definitions.** Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:
 - 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; Your failure to comply with your obligations as defined in the Agreement, including failure to pay valid past-due amounts or any suspension of the Services due to Your credit worthiness; failures of the Your applications or any of your equipment not within the sole control of Rogers or a party under contract with Rogers to provide services in connection with the Agreement; Your acts or omissions or any use or user of the Object Store Services authorized by you; during an event of Force Majeure.
 - 1.2 Calendar Month/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 your support requests. 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 Emergency Maintenance – Emergency Maintenance means any maintenance activities performed to prevent potential failures to infrastructure on which your Services are connected or avoid a security breach that could compromise your Content. Where possible, and the situation allows for it, you will be notified by Rogers within twenty-four (24) hours of any such Emergency Maintenance.
 - 1.5 Incident Management – An Incident means an unplanned interruption to any part of the Object Store Service or reduction in the quality of the Object Store Service. An Incident can be created by you by 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.
 - 1.6 Incident Management Resolution – Incident Management Resolution means that the service has been restored as per the SLA and this resolution has communicated to you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.
 - 1.7 Infrastructure Refresh – All equipment manufacturer guarantees, warranties and service agreements are purchased by Rogers and maintained by Rogers. Rogers will refresh hardware as needed to support the Services.
 - 1.8 Move/Add/Change/Delete (MACD) Request – MACD means your requests which are 'add-ons', changes or compliment the Object Store 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.
 - 1.9 MyAccount Portal – The Rogers portal that you use to manage your user accounts, review billing information, open and review support tickets, purchase additional Services, and review your reporting.
 - 1.10 Object Store Availability - For you, Rogers will use its Platform Monitoring and Alarming system to poll the availability of the Object Store Gateway to the external network and the underlying storage.

- 1.11 Out of Service Condition means a condition whereby there is an Object Store Service outage, including any lack of Object Store Services Availability.
- 1.12 Platform Monitoring and Alarming – the infrastructure supporting the Object Store Services is managed by Rogers. Management of the Object Store infrastructure, physical hosts, switching, storage, and the tools used by Rogers to determine the availability of the Object Store Service, including 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.
- 1.13 Response - measured from the time you call or create an Incident ticket in MyAccount Portal to the time a Rogers employee updates the ticket, speaks to, chats, or emails you.
- 1.14 Rogers Support System - The tools used by Rogers to record and track all Service Requests and Incidents Requests as part of the Object Store service.
- 1.15 Scheduled Maintenance - Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected. You shall be given at least five (5) days advance notice of Scheduled maintenance activities. The details of the service window and your negative impact will be communicated to you in the notification.
- 1.16 Self-Service – Self Service means any operation carried out by you using an available tool provided by Rogers without submitting a ticket or contacting the Corporate Support Team.
- 1.17 Service(s) – Rogers' Object Store Service(s).
- 1.18 Service Request – Service Request means a request from you 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 you 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 you by an update to the Rogers Support System by the Corporate Support Team in the Rogers Support System.
- 1.20 Site - This means the physical location(s) in which your Object Store Services are made available by Rogers.

2. Term, Rates, and Charges

- 2.1 The term of each Object Store Service (each an “**Initial Service Term**”) is as set forth in the Agreement(s). These terms commence on the date of signature of the Agreement by you, or, if these terms are attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon expiration of the Initial Service Term, Object Store Services may be renewed for an additional period set forth in an Agreement to be added to this Agreement by way of amendment (a “**Renewal Service Term**”) or, if no amendment is executed, the Services 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**”.
- 2.2 The Fees for the Object Store Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Professional Service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Object Store Services by any third party or unauthorized person.
- 2.3 Consumption of Rogers Object Store is metered using a “High Water Mark”. This is the peak total amount of the service used in a Calendar Month. Once the peak is achieved, it remains at that level until the end of the Calendar Month when it is reset. The charges set out in the Product Quote represent the “High Water Mark”

GB rate for the committed rate term. You will be responsible for all usage charges incurred. Unless otherwise specified, there are no limits or restrictions on usage.

- 2.4 Monthly Recurring Charges are set out in any applicable Agreement, representing minimum charges and are invoiced monthly, in advance, on the first day of each month. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 2.5 Unless otherwise agreed to in writing by you and Rogers, Rogers reserves the right to commence billing you for the Object Store Services on the earlier of thirty (30) days following execution by you of the Agreement or amendment related to the Object Store Services or thirty (30) days after the Service Effective Date ("Billing Start Date"). 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 Start Date. Applicable Service Credits will be applied to your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 2.6 If you purchase 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.
- 2.7 Rogers reserves the right to change rates for any and all Object Store Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.
- 2.8 Upon the commencement of a Month-to-Month Renewal Term for Object Store Services, the rates for such Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges.
- 2.9 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

3. User Subscriptions types (Standard and Principle)

- 3.1 Access to the Services is configured for two (2) types of users as set out below. Your account will specify your user type. The two available user types are:
 - a) **Standard User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below:
 - Use of the Object Store resources.
 - b) **Principle User** – this user level gives a single user the right to access the Services and the additional privileges/responsibilities below:
 - Purchasing additional services through the "Buy More" function;
 - Adding Standard Users to the Services;
 - Responsible for keeping the account information up to date;
 - Responsible for providing current You contact information for Rogers automatic notification systems;
 - Responsible for receiving all notices from Rogers relating to the Services.

4. Your Responsibilities and Acceptable Use Policy:

- 4.1 You must use compatible software (purchased or acquired separately) to access your Rogers Object Store Service.
- 4.2 You must ensure that the version of your software is compatible with the version of Object Store offered by Rogers. Rogers will publish the version of Object Store and notify you of 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, technical, emergency or support personnel associated with the restoration of the Object Store Services due to you performing any changes to your own software.
- 4.3 You bear all risk associated with your use of the Services.
- 4.4 You are responsible to ensure that the Services are sufficient for your needs.

- 4.5 You are solely responsible to determine that your use of the Services is compliant with all laws and regulations applicable to you.
- 4.6 You agree to use the Services in compliance with all applicable laws and regulations, including, without limitation applicable privacy laws.
- 4.7 You agree not to use the Services:
 - 4.7.1 To violate or infringe on the rights of other customers;
 - 4.7.2 To use the Services to gain unauthorized access to or to disrupt in any manner any third-party service, device, data account or network;
 - 4.7.3 To spam or distribute malware;
 - 4.7.4 In any way that could harm the Services or impair other's users use of the Services;
 - 4.7.5 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.
- 4.8 To the extent required by applicable laws and your own business requirements, you shall retain connection logs, or any data required to identify any internal or other user of your own services hosted on the Services.
- 4.9 You are solely responsible for use of the Services by any individual to whom you may have provided your password(s) and any other means of access (such as SSH access keys, API, etc.).
- 4.10 You are solely liable for the consequences of the loss of any passwords and any other means of access to the Services.
- 4.11 You are responsible for providing appropriate staff to participate in troubleshooting incidents and service requests. During an incident or a service request you will actively participate in the resolution of the request. Any time spent waiting for communications from you may result in the severity of the ticket getting downgraded and the time subtracted from the resolution time.
- 4.12 You are responsible for coordinating all communications with any third party you have contracted to provide any type of support for your services.
- 4.13 You are responsible for maintaining strong password to access the Services in the Rogers MyAccount Portal. Changes to the access controls require the provision of your designated secure user name and password. Credentials designated by you must utilize strong security traits (e.g. upper and lower case values, numeric and non-numeric values). You are responsible for credentials and must keep credentials secure and confidential.
- 4.14 You shall be solely responsible for providing your services, technical support, pricing and service plans, billing and collections, and any and all other services to your end users, and Rogers shall have no obligations or liability whatsoever to end users in relation to the Object Store Services.
- 4.15 You 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. You agree to pay any such charges based on use of the Services by your end users.
- 4.16 In addition to the indemnification provisions set out in the Agreement you 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 you agree 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.
- 4.17 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.
- 4.18 Unless Rogers believes an immediate suspension of your Services is required, Rogers will use reasonable efforts to provide notice before suspending your Services.
- 4.19 The Services described herein are subject to additional license terms, with which you hereby agree to comply. Your use of Microsoft software is subject to Microsoft's End User License Terms, which are set forth at the link below.
[https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms\(WW\)\(ENG\)\(Apr2014\)\(CR\).pdf](https://myaccount.datacentres.rogers.com/legal/SPLA2013EndUserLicenseTerms(WW)(ENG)(Apr2014)(CR).pdf)
- 4.20 The Services will continue on a month-to-month basis after the end of the Term with the following conditions:
 - 4.20.1 You are responsible for making end of the Term arrangements by renewing your Services or cancelling the Services.
 - 4.20.2 If you do not make end of Term arrangements then Rogers may, in its sole discretion, terminate the Services.

5 **Your Indemnity.**

- 5.1 In addition to the indemnification provisions set out in the Agreement, you 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 you agree 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; and (iii) any third-party content.

6 **Backup, Content Integrity and Disaster Recover**

- 6.1 The Object Store Services do not backup or perform any data backup services of your Content as part of the Services.
- 6.2 You agree to take all the necessary measures to back up your Content in the event of data loss/Content loss or deterioration of your Content, whatever the cause.
- 6.3 For greater certainty, the inclusion of data replication (as part of resiliency) shall not be considered data backup services.
- 6.4 You are solely responsible to set up your own business continuity plan and/or business recovery plan.

7 **Services and Networking**

- 7.1 Object Store S3 Compatible API: You will manage your Content in the Rogers Object Store Service through the use of your acquired and managed software.
- 7.2 Network Access: The Services include access to a shared internet connection with a maximum throughput of 250Mbps. You will access the Services by way of this shared internet connection. If you require private or dedicated network access, you can purchase a Rogers Wireline service.
- 7.3 Ownership of Data Centre: You will under no circumstances be permitted to access the physical space or the surrounding facility from which the Object Store Services are performed. You 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 Object Store Services or your termination for any reason pursuant to the Agreement.
- 7.4 Data Centre Carrier Neutrality: Rogers will, in its sole discretion, allow third party network and access providers to provide connectivity to your Object Store Services. Rogers will provision the cross-connection between your colocation space and the third party connectivity provider. You are 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.
- 7.5 Fair Use of the Services: The Services are subject to fair use by you. Rogers will ensure that you do not disrupt the use of other users of the Services. Rogers will prevent Noisy Neighbours and will generally limit the ability of you to adversely affect other users and other Customers. Noisy Neighbor means you 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 you are a Noisy Neighbour Rogers may, and Rogers reserves the right to temporarily limit your use of the Services. Rogers will attempt to contact you prior to any corrective action. Any action by Rogers to address a Noisy Neighbour and any disruption to your Services is excluded from the SLA for the Services.
- 7.6 Client-Side Internet: The You will access the Services remotely via the internet. You must have your own local internet connection to access the Service, and is solely responsible for the aforementioned internet connection, in particular its availability, reliability and security.

8 **Security Access and Fraud**

- 8.1 You agree to implement and is solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Object Store Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Object Store Services, and your accounts, as well as for user access security or network access security with respect to your Content.
- 8.2 Rogers shall limit access to Object Store Services and take reasonable security efforts to prevent unauthorized access to the Object Store Service.
- 8.3 Rogers shall use commercially reasonable efforts to assist in network security breach detection or identification and prevent unauthorized access to Object Store Services. Where a situation is considered a security breach or could have serious consequences, Rogers shall notify you as soon as feasible and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.
- 8.4 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, Services and/or your data, or (b) your 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. You acknowledge that such suspensions do not release it of any obligation to pay for Services.
- 8.5 You are solely responsible for identifying all user management rules for the account and for user access security or network access security with respect to your Content and for establishing access and user management controls that clearly identify individuals who have access to account administration, security, technical and/or billing rights ("**Access Control and User Management Controls**") and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to your Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential. You are responsible for any use of the account regardless of who uses the Services.
- 8.6 Rogers will track all access to your Services through an online ticketing system and ensure that those who requested access have all your necessary documented approvals prior to accessing your Object Store Services. If Rogers cannot verify the your identity or suspects that there may be fraudulent or illegal activity Rogers may decline the request. In such an instance Rogers will attempt to contact the main or alternative contact.
- 8.7 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.
- 8.8 In the event of any emergency that presents a risk of an Out of Service Condition, or damage to your equipment or data belonging to Rogers, a third party, the Site or Rogers' data centre facilities, or to any persons or property present therein, Rogers may disable Object Store Services as is reasonably necessary to respond to the emergency; ; and only as necessary, Rogers may disable Object Store Services if the emergency requires such action to avoid damage.
- 8.9 You are not permitted to run security penetration tests on the Object Store Services without prior written approval from Rogers. Any such actions will be considered improper use under the Agreement. Rogers may, without liability, restrict Service access if you perform invasive platform testing without prior written approval from Rogers.

- 8.10 If Rogers detects or reasonably believes that your usage represents a security risk, an email will be sent to you, identifying the account(s) affected, and stating that a reinstallation procedure must be performed in order to maintain the integrity of the Instance and the entire infrastructure. In such case, Rogers reserves the right to suspend the Services immediately in order to maintain the integrity of your Content.
- 8.11 Manipulations consisting of transferring data from the affected system to the new system must be done by you. Rogers will provide reasonable assistance, as determined by Rogers, to you to install a new system but is under no obligation to meet all of your needs in this regard.
- 8.12 Rogers shall not be held responsible for Your usage of the Object Store API by the your application.

9 Support

- 9.1 When reporting an incident and creating a ticket for the purposes of technical support, you agree to provide Rogers with all relevant information reasonably required for the diagnosis and intervention of the incident.
- 9.2 You undertake 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 you to provide Rogers access to your Instance. If you are 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.

10 Software License Grant

- 10.1 Upon purchase of Object Store Services by you, Rogers will grant to you a license for Object Store.
- 10.2 Any licenses provided by Rogers to you for your Object Store Services are solely permitted for use upon the Object Store infrastructure. Upon termination of the Object Store Services for any reason, these licenses shall be terminated, and you shall have no further rights to the Software, except as necessary to comply with the Agreement. For greater clarity, "you" in the above paragraph shall also include all end users of the Services.
- 10.3 You will be required to provide your own application software licensing to be used with the Object Store platform. You agree that you have taken all necessary steps to ensure that the licenses being used are legally licensed and supported through an agreement between you and the software provider. You will, if required, provide proof of purchase for all your-provided licensing being used on the Object Store platform.
- 10.4 If you make use any non-Rogers provided software, you represent and warrant to Rogers that you have the right and applicable license to use the software in that manner.
- 10.5 If Rogers has agreed to provide management services, then you represent and warrant that your software license agreement with the software provider permits Rogers to perform these activities.
- 10.6 You are responsible for reporting to Rogers any changes to your use of the Services including but not limited to your Object Store, virtual machines, or software agreements that impact your compliance with any software EULA. If you fail to disclose such changes you are liable for any incremental software licensing fees incurred by Rogers from the time of the change

11 Content

- 11.1 Definition of your Content. Your Content is defined as any software (including machine images), data, text, audio, and video or images that you or any user transfers to Rogers for processing, storage or hosting by the Services in connection with your account and any computational results that you or any user derives from the foregoing through your use of the Services.
- 11.2 Your Content does not include account information. The terms of the Agreement or other agreement with us governing the use of Services apply to your Content.

- 11.3 Ownership of Content. All interest in and ownership of Content including, but not limited to, those portions of the Content that are your trade names, trademarks or service marks, are and shall remain the property of you
- 11.4 Rogers is only responsible for maintaining the environment with a level of redundancy in accordance with the Service Level Agreement. This redundancy does not extend to your applications that your Content on Object Store.
- 11.5 You shall remove all Content from the Object Store prior to the date of termination of the Object Store Services. In the event that the Content is not removed, such Content will be considered abandoned, and Rogers may, without liability to you, delete the Content.
- 11.6 If you have contracted for managed services with Rogers please refer to such other terms.

12 Product Service Level Agreement ("SLA")

- 12.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("**Service Credit**").

Table 1: Power Availability

	Power Availability	Objective	Service Level Credit
Object Store Availability	99.99%	<p>Poll Object Store 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.</p> <p>If the Object Store 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</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>
MyAccount Portal (MyAccount API and MyAccount Web Portal)	99.99%	<p>Poll every five (5) min. for connectivity to the MyAccount Portal and record a value of UP or DOWN.</p> <p>Impact = 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</p>	<p>99.99% to 99.85% Monthly = Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.</p> <p>Less than 99.85% Monthly = Rogers will issue a credit to you in an amount equal to the total monthly bill for the affected service monthly fee paid by you for the affected Services.</p>

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.	<p>Response Target Metric: When you call in live 24x7 = Live answer When a you create in MyAccount Portal = Two (2) hours</p> <p>Incident Management Resolution Target: Six (6) Hours</p>	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.
Incident Management – Severity 2	Response Time Target and Incident Management Resolution Target as	Response Target Metric: When you call in live 24x7 = Live answer	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of

	indicated below.	When you create in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Fourteen (14) Hours	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 you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours Incident Management Resolution Target: Seventy-two (72) Hours	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you of the cumulative duration of such unavailability during such Calendar Month.
Service Request	Response Time Target as indicated below.	Response Target Metric: When you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours Service Request Resolution Target: Five (5) Business Days (Monday to Friday 8am to 8pm EST)	Rogers will issue a credit to you in an amount equal to 1/30th of the total monthly bill for the affected service monthly fee paid by you 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 you call in live 24x7 = Live answer When you create in MyAccount Portal = Two (2) hours MACD Request Resolution Target: Scoping performed on a case by case basis	SLO Only (no service credit)

12.2 Incident Management Severity Levels (Table 2):

- 12.2.1 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 your Content is at a significant risk of loss or corruption; You have had a substantial loss of service; and Your business operations have been severely disrupted.
- 12.2.2 Severity 2: Major functionality is severely impaired. High impact; and Degradation of critical service or total of loss non-critical services
- 12.2.3 Severity Level 3 (S3) Partial, non-critical loss of functionality of the Services. Low impact – no direct business impact; and Non-critical services affected;
- 12.2.4 Service Request: A request from you 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).
- 12.2.5 Move/Add/Change/Delete (MACD) Request: Are requests which are 'add-ons' or compliment the Object Store 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.

12.3 Calculation for Response Time and Resolution Target (Table 2) for Incident Management (except if SLO):

- 12.3.1 Response Time Target Rogers response time will be measured from the time you call or create 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 you.

12.3.2 Rogers' resolution will be measured from the time you call or create an Incident ticket in MyAccount Portal (Rogers Support System) to the time a Rogers employee updates the Rogers Support System ticket informing you the incident is resolved.

12.4 Monthly Service Level Credit Limitation. 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.

12.5 Service Credit Request Process. If Rogers has failed to meet any of the above service levels for a particular Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.

12.6 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Object Store Services. you 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 you will be entitled to as outlined within this SLA.

13 Termination Fees.

13.1 If you terminate the Services without cause, or if Rogers terminates the Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

- a) One hundred (100%) 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 of 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;
- b) any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the applicable Service that exceeds the amount set out in (a) above; and
- c) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Service.

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

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

Dedicated Backup Service

The following terms pertain specifically to Dedicated Backup Service supplied by Rogers to you.

The Dedicated Backup infrastructure is co-located in the Primary Data Centre. Optional Geo-redundant Dedicated Backup includes replication of the backup data to secondary storage infrastructure, geo-diverse from your infrastructure. Dedicated Backup Service(s) ("**Services**") are available to both Rogers Colocation Rogers Private Cloud customers.

2. **Features.** Dedicated Backup Services include the following features:

- 9.1 Geodiversity Dedicated Backup (optional) Where requested by you, the Dedicated Backup Service is available with geodiversity, for an additional charge. Rogers will provide network transport and storage infrastructure in support of the geodiversity requirements. Rogers will replicate daily the backup data from the Primary Data Centre to the Geo-diverse Data Centre.
- 10.1 Backup Storage. The Dedicated Backup Services have a defined amount of backend (GB) capacity. The Services have a standard 1:3 ratio of frontend data (GB) to backend data (GB) for the standard 15-day retention. The realized ratio of frontend data (GB) to backend data (GB) may differ depending on your specific compression, deduplication, and any non-standard retention policies. If additional backend (GB) capacity is required to meet your requirements, Rogers will request you either reduce your retention policy, adjust the amount of data backed up, or recommend you acquire additional storage capacity at a fee. If you do not respond or take one of the above actions within 30 days Rogers may prioritize your most recent data which may result in data loss. Any such action will affect your contracted retention policy and specifically exclude any SLAs related to Section III, Part 3 of this document.
- 11.1 Standard 15 Day Retention Policy. The standard retention policy for servers, virtual machines, filesystems, and applications is fifteen (15) days. Daily backups are retained for seven (7) days. Once every seven (7) days a synthetic full backup is made and retained for an additional seven (7) days.
- 12.1 30 Day Retention Policy (optional). The retention policy for all servers, virtual machines, filesystems, and applications can optionally be specified to thirty (30) days. Daily backups are retained for 7 days. Once every 7 days a synthetic full backup is made and retained for an additional twenty-one (21) days. 30 days retentions should be sized at 1:5 of frontend to backend ratio at minimum.
- 13.1 Custom Retention Policy (optional). You can work with Rogers to create a custom retention policy that will make use of backend (GB) storage. Any such work is provided under a separate Statement of Work (SOW). Custom retention policies should be sized at 1:8 of the front end to backend ratio at a minimum.
- 14.1 Daily Backup Frequency The standard backup frequency for servers, virtual machines, filesystems, and applications is once every twenty-four (24) hours.
- 15.1 Long term storage (optional) Upon your request (ad hoc or on a recurring schedule) a synthetic full backup will be copied to Rogers Object Store Service located in Rogers CGY3 Data Centre. Standard Object Storage rates apply. See Rogers Object Storage terms for more information.
- 16.1 Supported Applications. Data can be data from a wide range of applications, including Windows file systems: Active Directory: Databases such as; Microsoft SQL, MySQL, Microsoft Exchange.
- 17.1 Data Encryption (optional): Backup data can be encrypted in transit and/or at rest. Encryption at rest is achieved using self-encrypted disks. Encryption affects the number of server resources required to perform the backups and must be scoped in at the time of contracting and prior to the Services being active. Additional charges apply for the additional services.

- 18.1 Backup Restoral. At your request, Rogers will evaluate the restore activity into two categories: if the restore is for less than ten percent (10%) of the total frontend (GB) data, then you can request up to two (2) restores for the protected data within a calendar month. If the restore is larger than 10% of the total frontend (GB) of data you can request one (1) restore per calendar month. Rogers will request a Restore Planning meeting with your designated Restore Prime. Rogers will ask to see your DR or recovery plan and will work together to plan out the restore activities. If you do not have a DR or recovery plan, you may accrue fees associated with duplicate restores or consulting work. You are responsible for providing a suitable storage target that includes connectivity and sufficient storage to recover the requested data set. All restores performed as part of this service are by default in-place restores.
- 19.1 Dedicated Backup Reporting. You will receive a daily email outlining the quantity of Dedicated Backup data per your system. Rogers will notify you in the event that your backend data exceeds eighty percent (80%) of the Dedicated Backup storage capacity.
- 20.1 Dedicated Backup Portal. You can initiate your own restores from a Rogers provided portal however, Rogers provides no change management support in the event that you initiate your own restore. All your initiated activities are logged.

3. **Definitions**. Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:

2.1 Acceptable Downtime. In calculating whether or not Rogers has met the commitments in any specific month lack of availability owing to downtime for any of the reasons set out below will not be factored into the SLA calculations: Scheduled Maintenance; your failure to materially comply with its obligations as defined in the Agreement, including failure to pay valid past-due amounts; order suspensions due to your credit worthiness; failures of your applications or your Equipment not within the sole control of Rogers or a party under contract with Rogers to provide services in connection with the Agreement; your acts or omissions or any use or user of the Dedicated Backup Services authorized by you; and during an event of Force Majeure, as described in the Agreement.

2.2 Backup Window: The portion of the day where backups can occur.

2.3 Business Day. Monday to Friday inclusive, excluding statutory holidays observed in the Province of Ontario.

2.4 Corporate Support Team. Corporate Support Team means the technical support group at Rogers' responsible for handling all support requests from you for the Dedicated Backup Services.

2.5 Dedicated Backup Availability. Dedicated Backup Availability means the percentage of time during a specific calendar month that the Dedicated Backup Services are available for your use, as set out in these terms. Dedicated Backup Availability is based on ticket information from Rogers Customer Care.

If an Out of Service condition is detected or reported, the Dedicated Backup Services will be deemed to be unavailable for the length of the Out of Service condition. Dedicated Backup Availability is calculated as the total number of minutes that the Dedicated Backup Services were unavailable during a specific month, divided by the total number of minutes in the specific month, multiplied by hundred (100) (for the percentage).

2.6 Geo-diverse Data Centre. A Rogers data centre location physically diverse from the Primary Data Centre

2.7 Power Availability. Power Availability means the percentage of time during a specific calendar month that the power supply to a particular Space is available. For redundant power configuration, failure of both A and B PDU circuit(s) at the same time will be considered an Out of Service condition for Power Availability. Power Availability is based on ticket information from Rogers Customer Care.

If an Out of Service condition is detected or reported on a specific power supply, the power supply will be deemed to be unavailable for the length of the Out of Service condition. Power Availability is calculated as the total number of minutes that the power supply was unavailable during a specific month, divided by the total number of minutes in the specific month, multiplied by hundred (100) (for the percentage).

2.8 Primary Data Centre. The Rogers data centre location in which both your infrastructure is located

2.9 Recovery Point. Recovery Point refers to the timestamp and quantity of your data available to restore. With Dedicated Backup Services, your data is backed up nightly. Therefore, you have recovery points related to your selected retention policies.

2.10 Scheduled Maintenance. Scheduled Maintenance means any maintenance activities performed during the backup window on the infrastructure to which your Services are connected provided that you shall be given at least forty-eight (48) hours' advance notice of such maintenance activities. Such activities are typically performed during the standard maintenance window on Tuesdays, Thursdays and Sundays from 12AM to 7AM local Time.

4. Term, Rates, and Charges.

3.1 The term of each Dedicated Backup Service (each an **"Initial Service Term"**) is as set forth in the Agreement(s). The term of this Schedule commences on the date of signature of the Agreement by you, or, if this Schedule is attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon expiration of the Initial Service Term, a Dedicated Backup Service may be renewed for an additional period set forth in an Agreement to be added to this Agreement by way of amendment (a **"Renewal Service Term"**) or, if no amendment is executed, the Dedicated Backup 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"**.

3.2 The Fees for the Dedicated Backup Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Dedicated Backup Services by any third party or unauthorized person.

3.3 Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Monthly Recurring Charges set out in any applicable Agreement represent minimum charges. Unless otherwise specified, there are no limits or restrictions on usage.

3.4 Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.

3.5 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Dedicated Backup Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Dedicated Backup Services 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 your invoice within two billing cycles after Rogers approves your request for Service Credits.

3.6 Professional Services offered by Rogers to complete your specific requested work are subject to additional charges and require your approval of a Statement of Work. Applicable charges include, but are not limited to, travel, living and miscellaneous expenses. You will also be responsible for all costs associated with the purchase, lease and, or subscription of any software, hardware, or related equipment required to fulfill the services under a Statement of Work.

3.7 Rogers reserves the right to change rates for any and all Dedicated Backup Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.

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

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

4 Security Access and Fraud.

4.1 You agree to implement, and is wholly responsible for implementing, security precautions and practices in relation to the use of the Dedicated Backup Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Dedicated Backup Services including your accounts.

4.2 Rogers shall limit access to Dedicated Backup Services and take reasonable security efforts to prevent unauthorized access to the Dedicated Backup platform. You are solely responsible for End User access security or network access security with respect to your data.

4.3 Rogers shall use commercially reasonable efforts to reasonably 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. Rogers' access control management policies ensure that Dedicated Backup Services will utilize controls and logging through the online ticketing system in the "myAccount" portal. Upon implementation of the order, you will identify all user management rules for the account. This will include identifying which individuals have access to account administrative, security, technical and billing rights. Changes to the access controls require the provision of your designated secure username and password. Credentials designated by you must utilize strong security traits (e.g. upper and lower case values, numeric and non-numeric values). You are responsible for credentials and must keep credentials secure and confidential.

4.4 Rogers will track all access to your Services through the online ticketing system and will ensure that you have all your necessary documented approvals prior to accessing or changing your Services. When the situation is considered a security breach or could have serious consequences, Rogers will notify you and will act on your behalf if Rogers is unable to get correct approvals in a timely manner to deal with the threat.

4.5 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 Dedicated Backup Services if the emergency requires such action to avoid damage.

4.6 You agree to co-operate and assist Rogers with any investigation or action taken in relation to Rogers' operations and provisioning of services, confirmation of your compliance with the Agreement and, or breach of the Agreement by you.

4.7 You are not permitted to run security penetration tests on the Dedicated Backup Services without written approval from Rogers and any such actions will be considered improper use under the Agreement. Rogers may, without liability, restrict access to the Dedicated Backup Services if you perform invasive platform testing without written approval.

4.8 You are not permitted access to the physical space or the surrounding facility from which the Dedicated Backup Services are performed. You will not acquire any interest in, nor file any liens upon the Rogers Equipment, or any portion of the data centre as a result of the provision by Rogers of the Dedicated Backup Services or your termination for any reason pursuant to the Agreement.

5 Data Privacy

Except as otherwise set out in the Agreement regarding Rogers' right to access your information, only your authorized personnel can access your data in a readable form while it is housed on the Dedicated Backup platform. Rogers' personnel will perform administrative activities on the Dedicated Backup platform but will not have access to your readable data. Your data will be retained in Canada, at one of Rogers' secure data centre locations.

6 Encryption

Even where your data is encrypted, if Rogers is under a legal obligation to disclose certain information of yours', as described in the Agreement, Rogers is obligated to make the encryption keys available along with such lawfully requested data.

7 Product Service Level Agreement ("SLA")

7.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("**Service Credit**").

Table 1: Dedicated Backup Response Time

Method of Contact	Response Time per Incident (excluding Acceptable Downtime)	Service Credit
Telephone to Rogers Corporate Support Team	Immediate (ie. LiveAnswer)	one (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative sixty (60) minutes or fraction thereof, of Response Time, on a per Incident basis, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services for all Incidents in a particular month.
Ticket created in the MyAccount portal	2 hours	
Email sent to Rogers Corporate Support Team	4 hours	

Table 2: Recovery Point

Recovery Point	Rogers will create a Recovery Point for your data no less frequently than once per forty-eight (48) hours	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative twenty-four (24) hours or fraction thereof, of Recovery Point in excess of the SLA, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Services for all Incidents in a particular month.

7.2 You shall notify Rogers of any outage by opening a trouble ticket with Rogers within five (5) days for any Dedicated Backup Response Time misses (Table 1) and one (1) Business Day of any failure to meet the Recovery Point SLA (Table 2), following which Rogers shall validate the outage. If Rogers determines that there is an outage, Rogers will record it as an Out-of-Service condition in its system.

7.3 The combined cumulative total of all Service Credits for a calendar month for the Dedicated Backup Services will not exceed the total Monthly Recurring Charges for the affected Dedicated Backup Sites that Rogers has invoiced for such calendar month.

7.4 If Rogers has failed to meet any of the above service levels for a particular Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.

7.5 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Dedicated Backup Services. You 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 you will be entitled to as outlined within this SLA.

8 Termination Fees

8.1 If you terminate the Dedicated Backup Services without cause, or if Rogers terminates the Dedicated Backup Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

- a) One hundred (100%) percent of the average monthly charges per terminated Dedicated Backup 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;
- b) any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the applicable Dedicated Backup Service that exceeds the amount set out in (a) above; and
- c) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Dedicated Backup Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Dedicated Backup Service.

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

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

Cloud Backup Services

The following terms pertain specifically to Cloud Backup Services supplied by Rogers to you.

Cloud Backup Service(s) ("**Services**") are available to you if you have purchased Rogers Cloud Backup Services at an eligible Rogers data centre or if you who have purchased Rogers Private Cloud Services or Rogers Public Cloud Services.

1. **Features.** Cloud Backup Services include the following core and optional features:

- 1.1 Cloud Backup Storage. Cloud Backup includes an initial full backup of your data to one of Rogers' owned data centres. From that point on incremental backups are taken. Each day an incremental backup is taken. On day 7 the 6 daily backups are rolled up into a synthetic weekly full backup. At the end of 4 weeks the 4 weekly backups are rolled up into a monthly backup. Your data is kept for a pre-determined retention period and Rogers will begin to restore it to you when you log a LiveAnswer request with Rogers Corporate Support Team during that retention period.
 - 1.2 Cloud Backup with Geodiversity. Where requested by you and for an additional charge as set out in the Agreement, the Cloud Backup Services are available with geodiversity, which refers to a second backup copy of your data that is transmitted and stored daily to a second Cloud Backup location in a second city.
 - 1.3 Cloud Backup Data Retention. Cloud Backup Services are available in one standardized retention period: 14 days. At the end of the retention period your data "ages out" and is no longer available to you for restoration.
 - 1.4 Cloud Backup Supported Applications. Cloud Backup Services can be used to backup data from a wide range of applications, including: Windows File System; Linux File Systems; Active Directory; Databases such as MS SQL, MySQL, PostgreSQL, Oracle, Lotus Notes Database, and SAP; MS Exchange (server and mailboxes); MS Sharepoint; and Lotus Notes Documents. You are encouraged to contact your Rogers' representative to determine if your specific application(s) can be backed up using Cloud Backup Services.
 - 1.5 Cloud Backup Encryption Options. A unique encryption key is generated by the Rogers Cloud Backup platform for each backup and is required in order for restored data to be readable.
 - 1.6 Cloud Backup Restoral Options.
 - 1.6.1 VM Snapshot back up restores:
 - 1.6.1.1 In-Place Restore: this method will overwrite the original virtual machine. VM snapshot backup restore out of place within customer cloud environment. Cloud Environment must satisfy resource/space requirements for the out of place restore to occur.
 - 1.6.1.2 Out-of-Place Restore: restore the new virtual machine in parrel – Client must have enough resources for the size of the new machine, ram and compute.
 - File-Level Restore – via data agents: This option will either restore data in place to existing machine, or restore data onto existing machine
 - 1.7 Cloud Backup Reporting. You will receive a daily email outlining the quantity of Cloud Backup data per your system. Historical data reporting is available on the myAccount portal.
 - 1.8 Cloud Backup Portal. Effective October 2016, an enhanced customer portal will be made available to Cloud Backup customers. This portal will provide:
 - improved reporting, including logs, usage and metadata;
 - the ability for you to initiate your own data backup;
 - the ability for you to initiate your own data restore.
2. **Definitions.** Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:

- 2.1 Acceptable Downtime. means any of the following events: Scheduled Maintenance; Emergency Maintenance; your breach of the Agreement; order suspensions due to your credit worthiness; failure of your applications or your equipment not within the sole control of Rogers or its subcontractors; any act or omission by you or user of the Colocation Services authorized by you; any event of Force Majeure.
- 2.2 Business Day. Monday to Friday inclusive, excluding statutory holidays observed in the Province of Ontario.
- 2.3 Cloud Backup Availability. Cloud Backup Availability means the percentage of time during a specific calendar month that the Cloud Backup Services are available for your use, as set out in these terms. Cloud Backup Availability is based on ticket information from Rogers Customer Care. If an Out of Service condition is detected or reported, the Cloud Backup Services will be deemed to be unavailable for the length of the Out of Service condition. Cloud Backup Availability is calculated as the total number of minutes that the Cloud Backup Services were unavailable during a specific month, divided by the total number of minutes in the specific month, multiplied by hundred (100) (for the percentage).
- 2.4 Colocated Site means the physical Rogers data centre location in which Space for your equipment is made available by Rogers, as specified in the attached Agreement(s).
- 2.5 Corporate Support Team. Corporate Support Team means the technical support group at Rogers' responsible for handling all support requests from you for the Cloud Backup Services.
- 2.6 Emergency Maintenance means any urgent maintenance activities performed on the Rogers' infrastructure connected to your Space or your equipment in order to prevent or address imminent failures affecting Rogers' infrastructure.
- 2.7 Out of Service Condition means a condition whereby there is a Cloud Backup Service outage, excluding any Cloud Backup Service outage resulting from an Acceptable Downtime.
- 2.8 Power Availability. Power Availability means the percentage of time during a specific calendar month that the power supply to your particular Space is available. For redundant power configuration, failure of both A and B PDU circuit(s) at the same time will be considered an Out of Service condition for Power Availability. Power Availability is based on ticket information from Rogers Customer Care. If an Out of Service condition is detected or reported on a specific power supply, the power supply will be deemed to be unavailable for the length of the Out of Service condition. Power Availability is calculated as the total number of minutes that the power supply was unavailable during a specific month, divided by the total number of minutes in the specific month, multiplied by hundred (100) (for the percentage).
- 2.9 Recovery Point. Recovery Point refers to the timestamp and quantity of your data available to restore. With Cloud Backup Services, your data is backed up during the nighttime. Cloud Backup Services will perform Recovery Points at the following intervals:
- One daily Recovery Point during the first 7 days of the Service Effective Date;
 - One weekly Recovery Point per week from the 8th day from the Service Effective Date until the end of the first month; and
 - One monthly Recovery Point for the remainder of the retention period.
- 2.10 Scheduled Maintenance. Scheduled Maintenance means any maintenance activities performed on the infrastructure to which your Services are connected provided that you shall be given at least forty-eight (48) hours' advance notice of such maintenance activities. Such activities are typically performed during the standard maintenance window on Tuesdays, Thursdays and Sundays from 12AM to 7AM local Time.
- 2.11 Space means a designated section of the Colocated Site where space of one or more equipment cabinets (or racks) are set-aside by Rogers for your equipment.

3. Term, Rates, and Charges

- 3.1 The term of each Cloud Backup Service (each an "**Initial Service Term**") is as set forth in the Agreement(s). These terms commence on the date of signature of the Agreement by you, or if these terms are attached to the Agreement by way of amendment, then on the date of signature of said amendment by you. Upon

expiration of the Initial Service Term, a Cloud Backup Service may be renewed for an additional period set forth in an Agreement to be added to this Agreement by way of amendment (a **"Renewal Service Term"**) or, if no amendment is executed, the Cloud Backup 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"**.

- 3.2 The Fees for the Cloud Backup Services, including the Monthly Recurring Charges and Non-Recurring Charges, are set out in the Agreement(s). Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Cloud Backup Services by any third party or unauthorized person.
- 3.3 Monthly Recurring Charges are set out in any applicable Agreement, representing minimum charges and are invoiced monthly, in advance, on the first day of each month. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement.
- 3.4 Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Cloud Backup Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Cloud Backup Services or thirty (30) days after the Service Effective Date in accordance with these terms. 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 your invoice within two billing cycles after Rogers approves your request for Service Credits.
- 3.5 Consumption of Rogers Cloud Backup Services is based on the total front-end storage to be protected by the Service. You purchase a quota of front-end virtual machine storage to be backed up. You will be charged overage fees if its back-end usage exceeds the expected fair use level for the default retention.
- 3.6 Rogers reserves the right to change rates for any and all Cloud Backup Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.
- 3.7 Upon the commencement of a Month-to-Month Renewal Term for a Cloud Backup Service, the rates for such Cloud Backup Service will be increased by twenty (20%) percent, based on the average of the previous three (3) months of monthly recurring charges.
- 3.8 You must pay invoices within thirty (30) days of the date of each Rogers invoice.

4. **Site Access.**

Ownership of Facilities. You will in no case be permitted to access the physical space or the surrounding facility from which the Cloud Backup Services are performed. You will not acquire any interest in, nor file any liens upon the Rogers Equipment, or any portion of the data centre as a result of the provision by Rogers of the Cloud Backup Services or their termination for any reason pursuant to the Agreement.

5. **Security Access and Fraud.**

- 5.1 You agree to implement and are solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Cloud Backup Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Cloud Backup Services, and your accounts. You are solely responsible for End User access security or network access security with respect to your data.
- 5.2 Rogers shall limit physical access to the Site and use commercially reasonable efforts to assist in network security breach detection or identification and prevent unauthorized access to your equipment and as determined by Rogers, to identify security breaches. Where a situation is considered a security breach or could have serious consequences, Rogers shall notify you as soon as feasible and may act on your behalf if Rogers is unable to get correct approvals from you in a timely manner to deal with the situation. However, Rogers shall not be liable for any inability, failure or mistake in doing so, nor any security breach that occurs despite its

commercially reasonable efforts. Rogers provides absolutely no guarantees in relation to its efforts to identify security breaches.

- 5.3 You are solely responsible for establishing access and user management controls that clearly identify individuals who have access to your Space, account administration, security, technical and/or billing rights ("**Access Control and User Management Controls**"), to communicate same to Rogers, and to identify all user management rules for the account. You will inform Rogers in a timely manner of any change to your Access Control and User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The Access Control and User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to your Access Control and User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential.
- 5.4 Rogers will track all access to your Cloud Backup Services through an online ticketing system and ensure that those who requested access have all your necessary documented approvals prior to accessing your Cloud Backup Services.
- 5.5 You agree to fully co-operate and assist Rogers in a timely manner with any investigation or action taken in relation to Rogers' operations and/or provisioning of Cloud Backup Services, confirmation of your compliance with the Agreement, and/ or breach of the Agreement by you.
- 5.6 In the event of any emergency that presents a risk of an Out of Service Condition, or damage to your equipment or data belonging to Rogers, a third party, the Colocated Site, or to any persons or property present therein, Rogers may rearrange your equipment as is reasonably necessary to respond to the emergency. Additionally, and only as necessary, Rogers may disconnect or remove your equipment if the emergency requires such disconnection or removal to avoid damage. Rogers shall use commercially reasonable efforts to notify you prior to rearranging, disconnecting or removing your equipment, and in any case will notify you thereafter.
- 5.7 You are not permitted to run security penetration tests on the Cloud Backup Services without Rogers' written approval and any such actions will be considered improper use under the Agreement. Rogers may, without liability, restrict Cloud Backup Services platform access if you perform invasive platform testing without Rogers' prior written approval.

6. **Data Privacy**

Except as otherwise set out in the Agreement regarding Rogers' right to access your information, you're your authorized personnel can access your data in a readable form while it is housed on the Cloud Backup platform. Rogers' personnel will perform administrative activities on the Cloud Backup platform but will not have access to your readable data. Your data will be retained in Canada, at one of Rogers' secure data centre locations.

7. **Encryption**

Even where your data is encrypted, if Rogers is under a legal obligation to disclose certain information of yours, as described in the Agreement, Rogers is obligated to make the encryption keys available along with such lawfully requested data.

8. **Product Service Level Agreement ("SLA")**

- 8.1 If Rogers fails to meet the applicable service levels outlined in this Section, subject to the conditions set forth therein, you shall be entitled to a service level credit ("**Service Credit**").

Table 1: Cloud Backup Availability

	Power Availability (excluding Acceptable Downtime)	Service Level Credit
Geodiverse Cloud Backup Configuration	100%	One (1) day of pro-rated monthly recurring charges for the impacted Cloud Backup Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Cloud Backup Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Cloud Backup Services.
Non-Geodiverse Cloud Backup Configuration	99.95%	One (1) day of pro-rated monthly recurring charges for the impacted Cloud Backup Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Cloud Backup Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Cloud Backup Services.

Table 2: Response Time

	Response Time (excluding Acceptable Downtime)	Service Level Credit (if Response Time not met)
Telephone to Rogers Corporate Support Team	Immediate (ie. LiveAnswer)	One (1) day of pro-rated monthly recurring charges for the impacted Cloud Backup Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Cloud Backup Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Cloud Backup Services.
Ticket created in the MyAccount portal	2 hours	One (1) day of pro-rated monthly recurring charges for the impacted Cloud Backup Services for each cumulative sixty (60) minutes or fraction thereof, of Out of Service Cloud Backup Services in excess of the SLA set out in Table 1 above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Cloud Backup Services.
Email sent to Rogers Corporate Support Team	4 hours	One (1) day of pro-rated monthly recurring charges for the impacted Cloud Backup Services for each cumulative sixty (60) minutes or fraction thereof, of Response Time in excess of the SLA set out in Table 1 above on a per Incident basis, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Cloud Backup Services for all Incidents in a particular month.

Table 3: Recovery Point

	Recovery Point (excluding Acceptable Downtime)	Service Level Credit
Recovery Point	At least once per forty-eight (48) hours	One (1) day of pro-rated monthly recurring charges for the impacted Cloud Backup Services for each cumulative twenty-four (24) hours or fraction thereof, of Recovery Point in excess of the SLA set out above, up to a maximum of fifty percent (50%) of the monthly recurring charges for the impacted Cloud Backup Services for all Incidents in a particular month

8.2 Outage Notification. You shall notify Rogers of any outage by opening a trouble ticket with Rogers within five (5) days for any Cloud Backup Availability issue of any Out of Service condition or Response Time misses and Business Data Centre and Cloud Terms

one (1) Business Day of any failure to meet the Recovery Point SLA, following which Rogers shall validate the outage. If Rogers determines that there is an outage, Rogers will record it as an Out-of-Service condition in its system.

8.3 Monthly Service Level Credit Limitation. The combined cumulative total of all Service Credits for a calendar month for the Cloud Backup Services will not exceed the total Monthly Recurring Charges for the affected Cloud Backup Sites that Rogers has invoiced for such calendar month.

8.4 Service Credit Request Process. If Rogers has failed to meet any of the above service levels for your particular Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.

8.5 Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Cloud Backup Services. You 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 you will be entitled to as outlined within this SLA.

9. Termination Fees

9.1 If you terminate the Cloud Backup Services without cause, or if Rogers terminates the Cloud Backup Services for cause, you shall pay to Rogers, as liquidated damages and not as a penalty, an amount which is equal to the sum of:

- a) fifty (50%) percent of the average monthly charges per terminated Cloud Backup 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;
- b) any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the applicable Cloud Backup Service that exceeds the amount set out in (a) above; and
- c) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Cloud Backup Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Cloud Backup Service.

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

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

Managed Cloud Connect Services

The following terms pertain specifically to Managed Cloud Connect Services supplied by Rogers to you.

1. **Definitions.** Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. The following terms, when capitalized, have the following meanings:
 - 1.1. **“Acceptable Downtime”** — means any of the following events: Scheduled Maintenance; Emergency Maintenance; your breach of the Agreement; order suspensions due to your credit worthiness; failure of your applications or your equipment not within the sole control of Rogers or your subcontractors; any act or omission of you or user of the Services authorized by you or any event of Force Majeure;
 - 1.2. **“Business Day”** — means Monday to Friday inclusive, excluding statutory holidays observed in the Province of Ontario.
 - 1.3. **“Charging Period”** — means the charging period applicable to the Service, as specified on the Agreement. If not specified on the Agreement, a monthly charging period applies.
 - 1.4. **“Downtime”** — means the percentage of time the Service is not running or available, calculated per Charging Period as the total number of minutes in the Charging Period less (Uptime plus Excused Downtime).
 - 1.5. **“Emergency Maintenance”** — means any urgent maintenance activities performed on the Rogers’ infrastructure connected to Space or your equipment in order to prevent or address imminent failures affecting Rogers’ infrastructure.
 - 1.6. **“End-user”** — means any person enabled, through a data connection over the internet, to access, use, purchase, download, or otherwise interact with your content, which is located on or distributed by means of your equipment.
 - 1.7. **“Excused Downtime”** — means the number of minutes in the Charging Period, rounded to the nearest minute that the service is ‘down’ due to:
 - i) acts or omissions of the you, contractors, or anyone you are responsible for;
 - ii) the acts or omissions of any third party, or the fault on a third party’s network;
 - iii) any failure, incompatibility, or error in the configuration of your equipment or cabling;
 - iv) Rogers’ suspension of the Service in accordance with the Agreement or the Acceptable Use Policy; or
 - v) an intervening event.
 - 1.8. **“Monthly Recurring Charge”** — means the monthly charge for the Service.
 - 1.9. **“Network”** — means Rogers owned and operated TCP/IP-based data communications network.
 - 1.10. **“Out of Service Condition”** — means a condition whereby there is a Service outage, excluding any Service outage resulting from an Acceptable Downtime.
 - 1.11. **“Scheduled Maintenance”** — means any maintenance activities performed on the Rogers’ infrastructure connected to Space or your equipment provided that you shall be given at least five (5) Business Days in advance notice of such maintenance activities.
 - 1.12. **“Service Credit”** — means a fee credit for unscheduled Downtime to the extent Rogers fails to meet the Service Availability target in a Charging Period.
 - 1.13. **“Statement of Work (“SOW”)** — means a document outlining the scope of a project to be completed by Rogers for you and describing the specifications and Professional Services required to deliver the Services.
 - 1.14. **“Service Availability”** — means the percentage of time the Service is running and available, calculated per Charging Period as Uptime divided by (the number of minutes in the Charging Period less Excused Downtime).
 - 1.15. **“Uptime”** — means the number of minutes in the Charging Period where the link state of the service is available, rounded to the nearest minute.
2. **Description.** Managed Cloud Connect Services (the **“Services”**) are a combination of Rogers provided professional services and connectivity, over hardware and software used to manage your cloud connection with virtual cloud routers and virtual edge routers accessible by virtual circuits and VPN respectively, using Internet Protocol in a highspeed multilateral peering environment.

The Services are made up of a combination of:

- 2.1. **IX (“IX”)** which is a high-speed multilateral peering service, delivered over the Service. Speed may be configured in 1Mbps increments, with a minimum speed of 50Mbps and a maximum speed equal to the port speed.

- 2.2. **VXC (“VXC”)** which is a high-speed point-to-point ethernet virtual circuit between two Services end points. Service speed may be configured in 1Mbps increments, with a maximum speed equal to the speed of the slowest point connected to the VXC.
- 2.3. **A Cloud Router (“Cloud Router”)** which is the software based virtual router on the network. It may be used to join two or more independent VXC Services into a single routing domain, providing Internet Protocol (“IP”) connectivity between all of the VXCs attached to that CR.
- i) The Cloud Router is available at selected data centres at fixed speeds of 100Mbps, 500Mbps, 1Gbps, 2Gbps, 3Gbps, 4Gbps, and 5Gbps. The speed specifies the aggregate bandwidth available to all the connected VXCs.
- 2.4. **A Virtual Edge (“Virtual Edge”)** is a software-based SD-WAN node IP router on the edge of the network which is accessible via VPNs over the public Internet. It provides virtual connectivity to other Services, as an alternative to the physical ethernet connectivity available via a Port in one of our data centres. It may be used to join your premises based SD-WAN nodes to each other, to other VEs, and to other Services offered on the network.
- 2.4.1. **Virtual Edge Prerequisites and Restrictions.**
- i) Virtual Edge must only be connected to validated SD-WAN equipment, and, to this end, you need to provide your own SD-WAN license key, alternatively purchase a license key via Rogers (if/when such license keys are made available by Rogers, Rogers being under no obligation to do so).
- ii) Virtual Edge is available at selected metropolitan areas to provide remote connectivity to your SD-WAN equipment, typically in those same metropolitan areas.
- iii) Virtual Edge is available in fixed sizes to accommodate small, medium and large customers. The size specifies the expected maximum data throughput and/or number of expected customer premises devices to connect. Sizing is based on specific workloads; actual throughput may vary based on your specific workloads. See Table 1 below:

TABLE 1: Virtual Edge

Size	Maximum Performance (throughput)	Maximum SD-WAN endpoints
Small (2vCPUs)	~250-500Mbps	~40
Medium (4 vCPUs)	~1 Gbps	~300
Large (8 vCPUs)	~ 5 Gbps	~600

- 2.5. **Professional Services.** Professional services, to the extent required to complete specific your requested work, are subject to additional charges and require your approval by separate SOW. Applicable charges include, but are not limited to travel, living, and miscellaneous expenses. You will also be responsible for all costs associated with the purchase, lease, and/or subscription of any software, hardware or related equipment required to fulfill the SOW.
3. **Service Level Agreement.**
- 3.1. **Service Level Commitment.** If Rogers fails to meet the applicable service levels outlined in Table 2 below, subject to the Service Credit Conditions set forth therein, you shall be entitled to a Service Credit.

TABLE 2: Service Availability

Description	Availability	Service Level Credit
Managed Cloud Connect Service Availability	99.995%	One (1) day of pro-rated monthly recurring charges for the impacted Services for each cumulative sixty (60) minutes or fraction thereof, up to 50% of the Monthly Recurring Charges for the impacted Services.

- 3.2. **Outage Notification.** Outage Notification. You shall notify Rogers of any outage by opening a trouble ticket with Rogers Customer Care within one (1) day for any Power Availability or Climate Control Availability and ten (10) days for any Network Availability of any Out of Service condition, following which Rogers shall validate the outage. If Rogers determines that there is an outage, Rogers will record it as an Out-of-Service condition in your system.
- 3.3. **Monthly Service Level Credit Limitation.** 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 Sites that Rogers has invoiced for such calendar month.
- 3.4. **Service Credit Request Process.** If Rogers has failed to meet any of the above service levels for your particular Site in any given billing month, you must contact Rogers and apply for a Service Credit within fifteen (15) 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 you.
- 3.5. **Service Credit Conditions.** The following conditions apply to Service Credits:
- i) where a Service Credit is available, the credit is the only remedy in the event of Rogers' failure to meet the Service Availability Target;
 - ii) you must apply for the Service Credit and cause your claim to be received within fifteen (15) calendar days of the end of the related Charging Period;
 - iii) the Service Credit can only be applied as a credit to your Managed Cloud Connect Services fees;
 - iv) the maximum Service Credit available for each Service in a Charging Period will not exceed one hundred percent (100%) of the total Monthly Recurring Charge for that Charging Period per said Service; and
 - v) Service Credits are not available if you have failed to pay for the Service when due and payable.

Notwithstanding the limitation of liability clause in the Agreement, the remedies set out herein are your sole and exclusive remedy for any failure or interruption in the Services. You 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 you will be entitled to as outlined within this Service Level Agreement.

4. **Service Terms and Conditions.**

- 4.1. **Term.** These terms commence on the date of signature of the Agreement by you, or inclusion of these terms to the Agreement by way of amendment and ends on the expiration of the last in force Service Term. The term of each Service (each an "**Initial Service Term**") is as set forth in the Agreement. Upon expiration of the Initial Service Term, a Service may be renewed for the additional period set forth in the Agreement to be added to this Agreement by way of amendment (a "**Renewal Service Term**") or, if no amendment is executed, the 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**".
- 4.2. **Fees.** The Fees for the Services, including the Monthly Recurring Charges are set out in the Agreement. Professional service charges are set out in any applicable Statement of Work. You are solely responsible in the event of charges arising from fraudulent and/or unauthorized use of your equipment, Rogers' equipment or Services by any third party or unauthorized person.
- 4.3. **Payment.** Monthly Recurring Charges are invoiced monthly, in advance, on the first day of each month. Such charges will commence as of the Service Effective Date. Any applicable Non-Recurring Charges shall be billable as of the date of execution of this Agreement. You must pay invoices within thirty (30) days of the date of each Rogers invoice. Unless otherwise agreed to in writing by Rogers and you, Rogers reserves the right to commence billing you for the Services on the earlier of thirty (30) days following execution by you of the Agreement related to the Services or thirty (30) days after the Space is made available to you by Rogers in accordance with these terms. In the first month, the charges will be prorated for the number of days in the month after the Service Effective Date. Rogers will, by way of invoice or otherwise, notify you of the Service Effective Date. Applicable Service Credits will be applied to your

invoice within two billing cycles after Rogers approves your request for Service Credits.

- 4.4. **Excess Usage Charges.** Monthly Recurring Charges set out in any applicable Agreement represent minimum charges. You are responsible for all charges for excess usage beyond the minimum Monthly Recurring Charges billed at a twenty-five (25%) percent premium above the monthly rate. Unless otherwise specified, there are no limits or restrictions on usage
- 4.5. **Rate Change.** Upon the commencement of a Month-to-Month Renewal Term for a Service, the rates for such Service will be increased by twenty (20%) percent, based on the average of the previous three months of monthly recurring charges. Rogers reserves the right to change rates for any and all Services throughout the Service Term upon the provision of ninety (90) days' written notice to you in the event of an increase in third party supplier costs.
- 4.6. **Termination.** If you terminate the Managed Cloud Connect Services without cause, or if Rogers terminates the Managed Cloud Connect Services for cause, you 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) any cost which Rogers must continue to pay to third parties for the remainder of the Initial Service Term or Renewal Service Term, as applicable, as a result of the early termination of the Service that exceeds the amount set out above; and
 - iii) a lump sum representing the amortized remainder of any waived or discounted installation or one-time charges associated with the terminated Service in consideration of your commitment to the Initial Service Term or Renewal Service Term, as applicable, for such Managed Cloud Connect Service.

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

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

- 4.7. **Service Assumptions.**
- i) You agree to implement and are solely responsible for security of your data and for implementing security precautions and practices in relation to the use of the Services. You are solely responsible for any non-physical security breach or unauthorized usage of the Services.
 - ii) You are solely responsible for establishing access and user management controls that clearly identify individuals who have access to your Space, account administration, security, technical and/or billing rights ("**User Management Controls**") and to communicate same to Rogers. You will inform Rogers in a timely manner of any change to User Management Controls, and shall be solely liable for any inconvenience, delay or damage that may result from any failure by you to do so. The User Management Controls will be such that the individuals being authorized to access as well as those authorized to perform any changes to User Management Controls use appropriate secure credentials such as secure usernames and passwords, which credentials must utilize strong security traits. You are solely responsible for credentials and must keep credentials secure and confidential.
 - iii) In using the Service, you will:
 - a) ensure that all frames forwarded to the Service:
 - b) use 0x0800 (IPv4), 0x0806 (ARP) or 0x86dd (IPv6) ethertypes;
 - c) have the same source MAC address;
 - d) are unicast only, excluding broadcast ARP packets and multicast ICMP v6 discovery packets;
 - e) not forward frames to the Service using the following protocols:
 - f) proxy ARP;
 - g) ICMP redirect;
 - h) link local protocols such as Spanning Tree and CDP; or
 - i) directed broadcasts;
 - j) not 'default route' traffic to an IX participant (another entity, user of the services) without your consent; and
 - k) not advertise any IP addresses allocated to the Service outside the IX peering network.

- iv) You acknowledge that each route advertised to the IX route server will point to the IX participant advertising that route.