BACKUP AND DISASTER RECOVERY SERVICES AGREEMENT

This Backup and Disaster Recovery Services Agreement ("**BDR Agreement**") applies to the provision of all Backup and Disaster Recovery Services provided by Optimus Tech Solutions Inc. ("**OTS**") to a client ("**Client**") pursuant to an Engagement Agreement (a "**BDR Engagement Agreement**"). This BDR Agreement is also subject to the Optimus Tech Solutions Standard Terms and Conditions ("**OTS Terms and Conditions**") which can be found here. To the extent of any conflict or inconsistency between the applicable BDR Engagement Agreement, this BRD Agreement and the OTS Terms and Conditions, the conflict or inconsistency shall be governed by the following in order of priority: firstly by the BDR Engagement Agreement; secondly, by this BDR Agreement; and thirdly by the OTS Terms and Conditions.

1. Term

This Agreement is effective upon the date of the applicable BRD Engagement Agreement and shall remain in force for a period of three years. The Agreement automatically renews for a subsequent one year term beginning on the day immediately following the end of the Initial Term unless either party gives the other sixty (60) days' prior written notice of its intent not to renew this Agreement. In the event of early termination Client is responsible to pay the monthly service remaining in the contract.

2. Fees

Client shall pay the monthly fees specified in the BDR Engagement Agreement within thirty (30) days of invoice. Adjustments for additional server(s) and/or workstation(s) or additional offsite storage will be applied in a prorated manner on the next billing cycle during the Agreement.

3. Services Provided

OTS shall provide an on-site Network Attached Storage (NAS) unit that acts as a local storage device and stand-by server in the event of server and/or workstation failure, including: (a) Incremental backups done on the NAS as frequently as every 5 minutes; (b) Secure Remote (Off-site) Storage provided at 1 datacentre; (c) Day to day data restoration of files, file folders, emails or email stores, SQL databases, and SharePoint; (c) Full data recovery from secure data centers with the most recent information stored offsite - in the event of total catastrophe, where the on-site server and NAS are lost; and (d) Full management, monitoring, and testing of the NAS and remote storage (collectively, the "**BDR Services**").

4. Security

All data is fully encrypted during transmit off-site and while stored off-site. All data is stored off-site, in encrypted form in secure datacentre facility. (a) Each file is encrypted using 256-bit AES and SSL key-based encryption technology. 256-bit AES encrypted data cannot be read without the corresponding keys, so encrypted data cannot be misused. (b) The on-site NAS unit communicates with off-site remote servers using SSL (Secure Socket Layers) technology. As a result, the online backup of data is encrypted twice. It is encrypted at all times using the 256-bit AES encryption, and it is encrypted again while it's being sent over the Internet. (c) Data stored off-site remains encrypted at all times.

5. Data Deduplication and Compression

Data deduplication and compression occurs prior to data storage and transmit using state-of-the-art technology. This ensures that backups are completed in a shorter timeframe, less storage space is used on the on-site NAS and at the off-site data centers, and needed bandwidth to transfer data off-site remains manageable.

6. Backup Frequency

Servers and/or workstations can be backed up as frequently as every 5 minutes. Retention policies can be customized to create as many archived versions of data and full recovery points as needed. Off-site backup frequency is continuous by default, and may be customized to meet Internet bandwidth limitations. Off-site backup frequency is ultimately depended on total data size, data changes, and available Internet bandwidth.

7. Smart Data Transport

Data transmission can easily be configured to minimize Internet bandwidth consumption. The on-site NAS and propriety off-site data transfer system leverages advanced bandwidth throttling to schedule Internet bandwidth used depending on the time of day, customized for each day of the week. This allows bandwidth to be limited during business hours to maintain network functionality and maximize bandwidth during off-peak hours to efficiently transfer data off-site.

8. Remote Storage provided at high availability Data Centre in Ontario

The BDR Services provide highly redundant storage in multiple redundant cluster nodes, including (a) Connectivity provided by multiple providers with automatic failover capabilities, (b) Facilities power supplemented with both battery backup and diesel generation capabilities, (c) Full physical security including global biometric authentication access methodology to track all authenticated data center personnel and prohibit the entry of any unauthorized persons, and (d) Fire suppression and environmental control.

9. Remote Storage and Base Remote Backup Image Creation

Client data is stored (in encrypted form) in located in Toronto, Ontario. (b) The initial backup will be sent via a SATA II drive to the primary remote storage facility. There is an approximately 2-week turnaround time to seed the initial backup off-site. Incremental backups will occur during the off-site seeding process and will collapse into the main backup once the off-site transfer is complete.

10. Recovery Time Objective (RTO)

OTS will log all retrieval activities from the Client. (a) OTS will attempt to resolve access, backup, or retrieval problems over the phone on first call within 24 hours of the first request. We can restore a file, file folder, email or an entire mailbox as needed. Please call our help desk for assistance. (b) In a

disaster, where you should lose your entire office, we will have a new NAS imaged, with the most current backup information-which is usually the previous day's data. It will be shipped out via next-business day air transportation to a location of your choice. When the NAS arrives, it is ready to be used as a virtual server. There is an additional cost for this service as declared in Section 13. (c) The NAS can also be used to perform a bare metal restore to dissimilar hardware which means that when a new server arrives, the NAS can be used to restore the most current data to the new server(s) and/or workstation(s) regardless of hardware.

11. Off-Site Virtualization

In a disaster where Client should lose your physical servers and NAS, servers and/or workstations may be virtualized off-site. (a) Servers can be virtualized in off-site data centre. There is an additional cost for this service as declared in Section 13. (b) Public IP and/or VPN access will be given to connect to remote virtual machines. Virtual machines can also be accessed using VNC and/or RDP.

12. Ownership of the Data

The backup data being stored on the NAS and at the Data Center remains the sole property of the Client. If the Client chooses to terminate services, OTS will assist Client in the orderly termination of services. This could involve copying the backup image to an external drive which can be synchronized with the data on the NAS. The Client agrees to pay OTS the actual costs of rendering such assistance.

13. Catastrophe Service

In the event of a catastrophe, fees for the "Disaster Recovery Service" will be as stipulated in the BDR Engagement Agreement plus applicable freight and shipment costs to deliver a new NAS that will contain the most current data loaded at the Data Center. Additionally, any service required to provide access to that data is included. The fees noted in the BDR Engagement Agreement will remain in effect and cover the costs associated with the new NAS. Fees for the "Off-Site Virtualization Service" for up to 30 days access to virtualized machines are stipulated in the BDR Engagement Agreement.

14. Loaned Equipment

Client agrees that the NAS unit utilized by OTS, in the execution of this service shall remain the property of OTS, and must be returned if requested. Client further agrees to cease the use of any technology that remains the property of OTS upon termination of this Agreement. If the NAS unit is stolen, damaged or destroyed, the client must pay current market prices at the time of the loss for a replacement unit.

15. Interference

Client shall not, directly or indirectly, during the term of this Agreement and for twelve (12) months following its termination, induce or influence any employee of OTS or any other person or entity to terminate their relationship with OTS.

16. Warranty

OTS warrants that the work will be performed to the best of its ability and in accordance with reasonable and customary practices prevailing at the time for its business. (a) As long as the monthly fees are current, the NAS unit is fully warranted and no additional charges will be incurred for hardware failure. Firmware and software updates are also included. (b) The NAS units cannot be modified in any way or the warranty and the management agreements are voided. This includes adding software applications to the NAS itself, adding memory and/or hard drives, etc. (c) NAS replacement parts will be shipped next business day air transportation and prepaid by OTS. (d) ALL WARRANTIES, WHETHER STATUTORY, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF QUALITY, DURABILITY, FITNESS FOR PARTICULAR PURPOSE, MERCHANTABILITY, CONTINUOUS USE, DESIGN, COMPLIANCE WITH APPLICABLE LAW, PERFORMANCE OR ERROR-FREE OPERATION ARE DISCLAIMED IN THEIR ENTIRETY.

17. Equipment and Facilities

Client agrees that OTS may utilize certain items of Client's equipment and may gain access to certain parts of Client's facilities. Client retains title and ownership in all of Client's equipment owned by Client and utilized by OTS, and must grant authority for OTS to access Client's facility. Facility access may be denied for any reason at any time, however if access to facilities is denied, Client understands that OTS may be unable to perform their duties adequately and if such a situation should exist, OTS will be held harmless.

18. Passwords

OTS acknowledges that it must have access to any and all systems and resources to perform their duties under this agreement. As such, it must have access to any and all passwords. Client should note that the backup data will always be encrypted and not accessible to anyone who does not have the password. If the encryption password is lost, the backup data will be inaccessible.

19. Termination and Additional Remedies

This Agreement may be terminated by The Client upon sixty (60) days' written notice if OTS: (a) Fails to fulfill in any material respect its obligations under this Agreement and does not cure such failure within thirty (30) days of receipt of written notice; (b) Breaches any material term or condition of this Agreement and fails to remedy such breach within thirty (30) days of receipt of written notice; (c) Terminates or suspends its business operations, unless it is succeeded by an assignee under this Agreement. OTS reserves the right to terminate this Agreement for any reason. If either party terminates this Agreement, OTS will assist Client in the orderly termination of services, including timely transfer of the services to another designated provider. Client agrees to pay OTS the actual costs of rendering such assistance.

20. No Third Party Beneficiary

Client shall not subcontract, assign, subrogate or transfer any interest, obligation or right under this Agreement without prior written consent from OTS, and any such attempt shall be null and void. Any dissolution, merger, consolidation, reorganization or transfer of a majority of the assets or shares of Client shall constitute an attempted assignment of this Agreement. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the parties and their successors or assigns.

21. Jurisdiction

This Agreement shall be governed by the provincial and federal laws applicable in Ontario, Canada.

22. Force Majeure & Malicious Acts

OTS shall not be liable for any loss, damage or failure due to causes beyond its control, including strikes, riots, earthquakes, epidemics, wars, fires, floods, weather, power failure, telecommunications and/or internet interruptions, the failure or closure of a financial institution, computer malfunctions, acts of God or any other failure, interruption or error not directly caused, or reasonably anticipated, by OTS.

23. Availability

For the purposes of calculating availability, OTS shall not be responsible for failures to provide service for any if the following exclusions exist: (a) Problems caused by resources on the clients network that interfere with the service. (b) Changes made to the client network not communicated to OTS. (c) Loss of internet connectivity to the client site for any reason. (d) Service failures that result from any actions or inactions of the Client contrary to IT Service's recommendations.

24. Travel Charges

Client is responsible for travel charges equal to 0.5 hours of the normal hourly rate for each on site visit by OTS.