This Service Schedule (the “Schedule”), between Sherweb Inc. (“Provider”) and You, the organization purchasing the Performance Cloud Platform and the Cloud Server(s) (“Service”), as identified as part of the subscription process for the Service (“You” or “Your”), is effective immediately and is issued pursuant to and incorporates by reference the terms and conditions of the Master Service Agreement (“MSA”) by and between Provider and You.

This Schedule includes the terms and conditions governing the Service provided to You under the Agreement. By accepting this Schedule between You and Provider - by checking the “I have read and accept the Terms and Conditions” box when completing the Account creation, by logging in on Provider administrative web Portal, or by placing an order for any of the Service, You agree to be bound by all of the terms and conditions set out in this Schedule. All capitalized terms in this Schedule shall have the same meaning as set forth in the MSA, unless defined herein. In the event of a conflict or inconsistency between the terms of the MSA and the terms of this Schedule, this Schedule shall supersede and govern.

1. Definitions. For the purposes of this Schedule, the following definition(s) apply:

“Cloud Server” means a virtual machine instance that runs its own operating system and sets of dedicated resources.

“Managed Service” means the Service managed by Provider as further described in Section 3 below.

“Performance Cloud Platform” means Provider’s application service used to manage Your Cloud Server(s).

“Service” means the Performance Cloud Platform and Cloud Servers.

2. Service

2.1. Subscription. During the Term, You may access and use the Service. Provider or its Third-Party Supplier retains all right, title, and interest in and to the Service, including without limitation all computers, other hardware, and software incorporated into or used by the Service, and this Agreement does not grant You any intellectual property rights in the Service or any of its components.

2.2. Storage Capacity; Data Transfer; Server Resources. If Your Account is allocated storage capacity and data transfer amounts on Provider’s servers according to Your Service Plan, this allocated storage size and data transfer can be increased through the Control Panel of the Portal for an additional charge up to the maximum amount allowed for each plan or service. If you consume more resources, additional charges will be added to your bill according to Provider’s standard price list. The Service may stop accepting, processing, or delivering data when the purchased limit is reached thus causing server unavailability or data loss. Provider shall not be held responsible for such unavailability or data losses. Your Cloud Servers are configured in such a way so the accounts are separated from each other to the maximum possible degree even if they share the same resource pool. However, Provider cannot be held responsible for any breach of security or data leak due to the shared environment.

2.3. Restoration. Provider recognizes that from time to time, Your End-Users or Administrative Users may mistakenly delete, in whole or in part, items in Your database, mailbox or public folders, as applicable. As this is not a system fault and restoration may require partial implementation of Provider’s disaster recovery procedures, Provider reserves the right to charge you, and you agree to pay for, restoration fees of 500$ USD per backup, plus taxes. Provider does not warrant the integrity of the content or mailbox or databases content, as applicable, of each individual backup.

2.4. Acceptable Use. Provider reserves the right to intervene on any Cloud Server if its behavior is affecting negatively the normal operations of Provider’s infrastructure, any other client’s Cloud Server or Provider’s reputation on other network or server. This intervention includes the suspension of Your Service in whole or in part. Provider will contact You as soon as reasonably possible regarding any issues related to this policy.
3. Managed Service

3.1. Description. If You choose to purchase Managed Service, Provider will provide You with the following features in connection with the Service: (i) Operating system configuration for Linux or Windows, including base configuration and hardening; (ii) Complete infrastructure setup; (iii) Security updates when available; (iv) Backup setup configuration; (v) Recovery testing of the backups at initial setup; (vi) Health monitoring of the Service; (vii) Performance evaluation (in accordance with Provider’s standard performance metrics) and making performance metrics available to you; (viii) Software installation & configuration at setup; (viii) Software updates upon availability; and (ix) Basic virus protection installation at setup (collectively referred as the “Managed Service Features”).

3.2. Limitation of Liability and Disclaimer. The Managed Service Features are provided on a best commercial effort basis. Furthermore, Provider reserves the right to refuse to perform any of the above features if it requires work in excess of the average workload for similar features for other clients, due to specific requirements that You may have. Provider makes no representation or warranty whatsoever regarding any of the above features and you agree that Provider shall not be liable to you for any loss or damage arising from the provision of the Managed Service Features, other than the rights and remedies that you may have under law for gross negligence or wilful misconduct. You further acknowledge that Provider offers no guarantee that any of your specific applications may be compatible or may interoperate with the Service and the features hereinabove.

3.3. Backup. Provider schedules daily backups of Your Data. Backups are monitored and checked for errors, and regularly scheduled tests of the restoration procedures are performed. Backup copy retention time is seven (7) days. Provider does not warrant, however, that a valid backup is available for every day of this period. If a disruption of the Service occurs, Provider will assign its highest priority and will make its best commercial efforts to ensure the timely restoration of the Service. Depending on the type of disruption that has occurred, Provider may elect to first restore the Service without the data. Any data not immediately accessible after a disruption in the Service will be restored from the most recent backup and made accessible with Provider’s highest priority. In order to ensure the readiness of Provider’s operators to complete the offline restoration process, Provider runs frequent drills to test restoration performance. Provider is not liable for data loss resulting from the failure or loss of backup media.

4. PCI-DSS Compliance Optional Services.

4.1. PCI-DSS Compliance Services. PCI-DSS compliance services can be added to the Service if You develop a cardholder environment or card processing service, helping to reduce the complexity of PCI-DSS certification. You may refer to Provider Performance Cloud’s PCI-DSS features in the relevant portions of your assessments for your certification.

4.2. Responsibility. Provider PCI-DSS v3.1 attestation of compliance (AoC) status does not automatically translate to PCI-DSS compliance for the services that You host on the Cloud Server. You are solely responsible for Your own PCI-DSS certifications. Provider may provide You with consulting services to help You configure and maintain Your services to meet PCI-DSS compliance requirements, and agrees to follow Your processes and requirements. These services include but, are not limited to, backups, audit log collection & analysis, managed security patching, firewall based intrusion detection system (IDS), anti-virus, and Windows PCI-DSS security template; for any services outside the list of the Infrastructure PCI-DSS scope, Provider will follow any reasonable customer processes requirements, provided that Provider is, in its own opinion, able to provide such services.

4.3. Limitation of Liability and Disclaimer. Provider makes no representation or warranty whatsoever regarding any of the services provided herein for PCI-DSS Compliance and you agree that Provider shall not be liable to you for any loss or damage arising from the provision of the PCI-DSS compliance services, other than the rights and remedies that You may have under law for gross negligence or wilful misconduct. PROVIDER MAKES NO REPRESENTATION OR WARRANTY REGARDING THE ABILITY OF THE SERVICES YOU HOST ON THE CLOUD SERVERS TO BE COMPLIANT WITH PCI-DSS NOR TO ACHIEVE ANY CERTIFICATION THEREOF. FURTHERMORE, YOU ARE RESPONSIBLE FOR THE SECURITY OF CARDHOLDER DATA provider POSSESES OR OTHERWISE STORES, PROCESSES, OR TRANSMITS ON YOUR BEHALF, OR TO THE EXTENT THAT THEY COULD IMPACT THE SECURITY OF YOUR CARDHOLDER DATA ENVIRONMENT.

5. Service Availability Warranty.

5.1. Service Availability. Provider covenants to a 99.999% Service Availability for the Service. For the purpose of this Schedule, “Service Availability” means the ability for an End-User, within an organization, to attempt access to a Cloud Server either through the Internet or directly from the Performance Cloud Platform.

5.2. Service Credit. Any Service Credit request shall, in addition the information set forth in the MSA, indicate the Cloud Server(s) affected by the Service Outage. Any Service Credit shall be calculated based only on the Cloud Server affected by the Service Outage.