PRIME NETWORKS
CONNECTED SECURED MANAGED

SCHEDULE TO THE MASTER SERVICE AGREEMENT

This Schedule forms part of the signed Master Service Agreement dated as amended from time to time between us (the 'Agreement') and is to be read in conjunction with that Agreement.

Additional Terms and Conditions

BACKUPS

1.1 The Service Provider will institute procedures by which, so far as reasonably practicable, securely encrypted copies of the Client's Company Data which will be taken automatically at intervals throughout the day and night and transmitted to and stored on the backup servers in purpose-built data centres, so as to enable access thereto by the Client in case of need.

1.2 Maintaining an up to date backup may require the Service Provider to base software in the Client's Location. All rights in any such software remains the property of the Service Provider, and on termination of this Schedules for whatever reason, we shall be entitled to uninstall it.

1.3 It is the Client's responsibility to maintain its own internet connection of adequate capacity to enable backup data to be transmitted to the backup servers. The data traffic required to maintain an up to date backup will consume bandwidth and may have a detectable negative effect on the overall performance of the Client's internet connectivity. The Service Provider shall not be liable for any internet connectivity issues during the backup process.

1.4 Unless agreed otherwise in writing, the Service Provider will generally maintain the following backups:

1.4.1 all backups taken over the preceding 24 hours
1.4.2 the last backup per day taken over the preceding week
1.4.3 the last backup per week taken over the preceding 4 weeks
1.4.4 the last backup per month taken over preceding 12 months.

1.5 So far as reasonably practicable, the Service Provider will review system backup logs on a daily basis and rectify any repeat issues that relate to problems at the Service Provider's data centres, storage devices or servers. It is the Client's responsibility to monitor its daily backup logs and this may mean that it is necessary for the Client tc take a fresh backup before the integrity of the backup is restored. It is the Client's responsibility to deal promptly with any queries the Service Provider raises, and to satisfy itself from reviewing backup logs itself that all data the Client wishes to be backed up is in fact included in the backup.

1.6 Whilst reasonable efforts will be made to ensure that a current backup is maintained of all relevant Company Data, the Service Provider cannot guarantee that all such data files will be 100% up to date at all times. Access to and restoration of an effective backup of Company Data depends on an up to date copy of the data being held on the backup servers. The backups are taken as periodic 'snapshots', and not continuous. Copying to backup can be delayed for a variety of reasons, e.g. a file may be locked by a user application whilst in use, and so not accessible to the Service Provider's backup software until the data file is closed by the user application; or there may be a third party communications failure, which delays transmission of a backup to the Service Provider's server. Data files actually in use at the moment disaster strikes are particularly vulnerable to this problem. The Service Provider's obligations are limited to using reasonable efforts to maintain an adequate recent backup, and to providing prompt access to such backup data is as in fact available.

1.7 Access to Company Data is obtained by the Client's users using their own PC terminals and internet connections. It is the Client's users' own responsibility to provide and maintain a sufficiently fast and reliable internet connection; support in relation to that connection is not included under this Agreement or the Schedules to this Agreement from time to time.

1.8 Such access, as clause 8.7 above, is obtained by user password; it is the Client's responsibility to keep any passwords issued to it for the Client's users secure, and to advise the Service Provider immediately if the Client has reason to suspect a password to have become compromised. All access using a password allocated to the Client is conclusively presumed to have been authorised by the Client.

1.9 So far as is reasonably practicable, backups will continue to be taken and Global Company Data Access will be available on a 24 hour 7 day basis; it is however technically impossible to provide fault-free service, and the service is provided 'as is' and without warranties of any kind, express or implied (other than warranties not capable of exclusion). Whilst the Service Provider will use reasonable efforts to ensure that service is maintained at all times, to keep unavoidable interruptions to a minimum, and to give notice of anticipated interruptions, it is inevitable that there may be times when the service or some aspects of it are not available. The Service Provider shall not be liable for any disruptions or interruptions in service.

1.10 The Client is aware that and accepts that online back up is not insurance against data loss, and nor is it a substitute for such insurance. Online back up is a service intended to help the Client take reasonable precautions to prevent data loss, at reasonable cost, and to gain access to backed up data so as to enable 'business as usual' as quickly as possible, in case of need.

SERVICE LEVELS

· Full data copy – the Service Provider will provide a full copy of the Client's data on an external drive within 4 hours for Clients whose Location(s) are based inside the M25. For Clients with more than 50GB of data, this will be extended to four hours plus the time taken to make a copy of the data to an external hard disc. There will be a one-off charge to cover the cost of the storage device or disc provided plus courier costs which shall be notified to Client's by the Service Provider from time to time.

· Mapped Drive – the Service Provider will provide a full copy of the Client's data via a Windows Terminal session, available over the internet within four hours. For customers with more than 50GB of data, this will be extended to 4 hours plus the time taken to copy the Client's data to the Windows Terminal session.

· Global Company Data Access – the Client shall have direct access by password to its Company Data backup at any time, to enable direct access and selective restore.

Kingsway House
103 Kingsway, London WC2B 6QX
Tel: 0207 443 5618- Fax: 0844 967 7777
Web: www.prime-networks.co.uk
REGISTERED IN ENGLAND 8403368