Statement of work for WiTCOM MPLS VPN

1. GENERAL

WiTCOM Wiesbadener Informations- und Telekommunikations GmbH (hereinafter referred to as WiTCOM) offers its business partners the service “WiTCOM MPLS VPN“ based on the “General terms and conditions of business of WiTCOM GmbH“.

2. STANDARD SERVICES

The “WiTCOM MPLS VPN” service enables companies to establish a private company network on the basis of MPLS (Multi Protocol Label Switching) technology across all sites.

Here, information is not transferred via the public domain of the Internet, but in a closed private network. Each MPLS VPN customer data traffic is fully separated from that of other WiTCOM customers. The WiTCOM MPLS network is connected to the network of the forwarding carriers by L2TP (Layer 2 Tunnelling Protocol).

2.1 Basic service

WiTCOM basic services include

- the provision of an access to the MPLS VPN backbone at each customer site;
- a virtual private data line (VPN) for direct communication of IP packets between customer sites;
- full installation and configuration of the VPN and the provision of all required network termination units to the customer for the contract term;
- support for this service;
- fault report hotline available day and night on seven days a week as outlined in point 5.1.

2.2 WiTCOM MPLS LINK BASIC/PREMIUM variant

WiTCOM MPLS LINK is a point-to-point or point-to-multipoint connection avoiding the public Internet. WiTCOM MPLS LINK is the ideal solution to interconnect sites of differing sizes. By using the BASIC and PREMIUM service levels you choose the availability and quality of service of your connection to the company network per site.

2.3 WiTCOM MPLS ACCESS BASIC/PREMIUM variant

WiTCOM MPLS ACCESS provides access to your company network using WiTCOM MPLS VPN. The access can optionally be realised by using an existing Internet access or one that is commissioned by the customer and hence lies in the responsibility of the customer. WiTCOM MPLS ACCESS is the ideal solution to connect small sites/subsidiaries to the company network. By using the BASIC and PREMIUM service levels you choose the availability and quality of service of your connection to the company network per site. WiTCOM ACCESS availability here only relates to the VPN line, and does not refer to the Internet access used by the customer.

2.4 WiTCOM MPLS REMOTE variant

By using WiTCOM MPLS REMOTE you provide your field service or home office workers with access to your company network from anywhere in the world. Please refer to point 3.2 for additional services.

2.5 Private data line for direct communication in the WiTCOM MPLS network

WiTCOM provides the customer with an IP/MPLS based high-speed network connecting the individual customer sites to the central WiTCOM network node. Data traffic between the customer sites is routed via the WiTCOM access network and the WiTCOM wide area network as well as the network of select partners, if required.

The IP/MPLS technology used in the WiTCOM access network allows the provision of a defined service quality for the customer. The connection between the customer site and the first active network element of the WiTCOM network is realised by a paired copper wire typically used by the relevant customer site only. In deviation hereof, within the WiTCOM coverage area the connection of a site can also be realised using WiTCOM own fibre optics or copper cable infrastructure.

2.6 Transfer interface

The point of transfer to the customer is a LAN interface in form of RJ-45 10/100 BaseT (Ethernet, Twisted Pair) to be provided at the network termination.

2.7 IP addresses

The IP addresses required for location identification are part of the scope of services and will be provided by WiTCOM for each customer site. The IP address space used will be determined upon consultation with the customer.

2.8 Access procedures and authentication

The access equipment (network termination) and the WiTCOM MPLS backbone use PPPoE (Point-to-Point Protocol over Ethernet) for DSL connections. For these connections the network termination provided by WiTCOM will be assigned a user name and password for authentication. Authentication typically uses CHAP (Challenge Handshake Authentication Protocol), otherwise PAP (Password Authentication Protocol) as well as access identification data for a Radius server contingent on the DSL access version used at the customer’s site.

For Ethernet connections and standard fixed lines the access to the MPLS backbone is fixed; session related authentication is not required.

2.9 Availability

The “availability of a service” is defined by the percentage share of a calendar year during which the service was not affected by any failure.

The availability is calculated according to the following formula:

$$\text{availability} = 100\% - \frac{\text{accumulated fault clearance times per calendar year in hours x } 100\%}{\text{calendary ear in hours}}$$

The availability (% p.a.) will be determined for the entire service, and the failures will be considered each with their fault clearance times measured according to 5.3.

WiTCOM MPLS VPN service availability is not below 98.5% p.a. in the basic version, and not below 99.5% in the premium version.

For relevant details please refer to the notification of readiness.

2.10 Network termination

WiTCOM MPLS VPN includes the provision of a Layer 3 (L3) based network termination per site for the contract term. Typically, here an IP router is used. The network termination unit requires 230V power supply and provides by default an RJ45 port with a 10/100BASE-T (Fast-Ethernet) or 1000 BASE-T (Gigabit-Ethernet) copper interface.

Dependent on the access version and bandwidth chosen, the network termination can be a desktop or 19" rack unit. WiTCOM will provide the network termination with a basic configuration.

3. ADDITIONAL SERVICES

WiTCOM specifically renders the following additional services each upon agreement and subject to technological and operational feasibility against separate payment.

3.1 Quality of Service

On the customer's request four defined service classes are available to prioritise the data packets within the WiTCOM MPLS VPN backbone.

These service classes are in declining priority (i.e. class 1 = highest priority, class 4 = lowest priority):

- Class 1: Real time data (streaming)
- Class 2: Voice data
- Class 3: Premium data (e.g. SAP)
- Class 4: Normal / other data

WiTCOM will agree the quality parameters of the service classes in coordination with the customer and realise them between the integrated MPLS VPN sites subject to technological feasibility.

WiTCOM will determine the detailed classification of the data packets in consultation with the customer. Here, WiTCOM MPLS backbone supports the following methods:

- Classification by the criteria "IP origination address", "IP destination address", IP type of service field (ToS)", "TCP/UDP port number or port ranges" as well as ("Destination port number or port ranges")
- "DiffServ" mechanism (DSCP Differentiated Services Code Point)
- "NBAR" mechanism (Network Based Application Recognition)

Non-classified data packets are sent in the lowest priority quality class by default.

3.2 WiTCOM MANAGED FIREWALL

On the customer's request, firewalls will be activated at the transfer points of the customer's company network to the WiTCOM MPLS backbone between the router and the internal network hardware of the customer. This will even increase the safety of the customer network. The hardware firewalls ensure a safe end-to-end encrypted supply tunnel between the local networks. VPN data to be transferred will be hard-coded and provide highest level security using the latest methods (such as AES, Advanced Encryption Standard). They are therefore protected against data theft and manipulation. WiTCOM will configure and manage the hardware firewall in coordination with the customer. This coordination is absolutely necessary if the customer wishes to make additional use of the available service classes (see 4.1) for Quality of Service reasons.

WiTCOM MPLS REMOTE requires the product WiTCOM MANAGED FIREWALL for dialing-in to the MPLS network with a software client.

3.3 Backup via parallel DSL line

On the customer's request select or all sites will be connected to the MPLS network over a parallel DSL connection. This backup connection will be established via another provider to clearly raise the availability of these locations. If the primary connection is interrupted at a certain location, the data link will be routed over the second parallel DSL connection.

3.4 Central Internet Gateway

On the customer's request, WiTCOM will set up a central Internet gateway for the customer. This gateway will handle the complete data traffic from the MPLS VPN network to the Internet. The customer determines the policy to be applied for Internet transactions of the users. WiTCOM will configure and manage the central Internet gateway.

3.5 Other services

On the customer's request additional services can be provided. They include the integration of an ASP (Application Services Provisioning) environment, or the customer's VoIP telephone system into the WiTCOM DATACENTER.

4. DELIVERY

4.1 Requirements

To install a "WiTCOM MPLS VPN", an operable network access must be available. WiTCOM provides the customer with one network connection each per site.

By default, the network access of the customer sites is provided by symmetrical connections to the Internet (e.g. "WiTCOM BASIC INTERNET ACCESS"). Alternatively, select sites can also use asymmetric DSL lines, Ethernet accesses, or standard fixed lines. Mobile users can be integrated over cellular data connections (UMTS/EDGE) or VPN dial-in to the MPLS VPN.

For the WiTCOM MPLS ACCESS variant an available network access is required at the customer's site. The customer is responsible for the provision of this access.

4.2 Realisation

For the realisation of the WiTCOM MPLS VPN, a technically cleared order shall be provided.

An order for the provision of WiTCOM MPLS VPN services is deemed to be technically cleared when the above requirements are met and the available infrastructure resources have been tested by WiTCOM delivering a positive result.

WiTCOM will make an on-site inspection, if required.

4.3 Standard installation

After completion of the installation works WiTCOM will inform the customer in writing (by e-mail or fax) of the operational readiness and request the acceptance of the service provided. Acceptance is deemed to be tacitly given if the customer fails to report any considerable deficiencies or to expressly refuse acceptance within five (5) work days at the latest after having been notified of the operational readiness. At the beginning of this term WiTCOM will again point out to the customer that failing to report any deficiencies or to expressly refuse the acceptance shall be deemed as acceptance upon expiry of the term. WiTCOM will install a connector in the immediate vicinity of the service line panel (HAK - Hausanschlusskasten).

At either end WiTCOM will install a network termination intented to terminate the WiTCOM MPLS VPN. The network termination serves as a connecting unit for customer terminals.

In the PREMIUM variant WiTCOM will install the network termination at the customer's location. WiTCOM is responsible for the configuration of the router on commissioning and during live operation.

Alternatively, for select sites an agreement can be reached that the routers will be provided and installed by a WiTCOM authorised company, or that the preconfigured routers will be mounted by the customer itself.

5. TECHNICAL SUPPORT SERVICES

WiTCOM will clear any faults in its technical equipment subject to technological and operational feasibility. Here, WiTCOM in particular renders the following services:

5.1 Fault reporting

WiTCOM is available to take fault reports from 0 to 24 hours a day under the technical hotline number 08000-948266 (08000-WiTCOM). When notifying the fault, it is important to report the following information to WiTCOM: service ID, company name, contact partner, location, if applicable (in case there are several locations) and the failure details.

5.2 Technical service availability

For WiTCOM MPLS LINK the technical service availability is 24 hours a day.

5.3 Fault clearance time

The fault clearance time starts when the fault report is received and ends when WiTCOM has remedied a service. It includes the response time. For a standard case WiTCOM guarantees a fault clearance time of eight (8) hours in the WiTCOM own network as well as for the PREMIUM variant, and twenty four (24) hours in the network of suppliers as well as in the BASIC variant.

The terms are deemed to be met if the complete recovery of the contractually agreed scope of service is completed within the fault clearance hours, and if notification was submitted as outlined in section 5.6.

Within the bounds of its possibilities the customer shall support WiTCOM in locating the fault, and, if required, grant access to its sites.

Special conditions of the fault management including a more detailed description of the process can be settled under a separate agreement as a supplement to the contract.

Fault clearance hours do not include:

- time periods during which the customer cannot be notified of the fault clearance by WiTCOM;
- time shares which result from lacking or insufficient customer co-operation during fault clearance.
- This applies in particular for the WiTCOM service technician's waiting times attributable to the customer in accessing the premises which might accommodate affected technical installations.
- delays which have been caused by circumstances lying beyond WiTCOM's control, e.g. in or by customer or third-party network operators' facilities.
- times in which the customer's network access at the WiTCOM MPLS ACCESS is at fault;
- delays which are due to acts of God (e.g. natural disasters).

5.4 Response time

The response time shall not exceed 30 minutes upon receipt of the fault information.

The response can also be performed by the appearance of a service technician at the customer's location.

5.5 Preliminary information

WiTCOM will inform the customer on the work status and further prospected measures on request every two (2) hours upon expiry of the response time or upon consultation.

5.6 Notification of completion

WiTCOM will notify the customer when the fault clearance is completed. If the customer cannot be reached on the first attempt, the fault clearance time as set out in point 5.3 shall be deemed as being met. Further notification attempts will be regularly performed.

5.7 Maintenance

WiTCOM shall inform the customer about scheduled maintenance works causing operational interruptions at least 10 work days in advance (Mon. - Fri. except for public holidays in Hessen). WiTCOM will consider the customer's interests when performing the maintenance works. Therefore, the works are to be performed preferably at times when the utilization of the services is low. The times for maintenance works are not taken into account when determining the availability.

5.8 Arrangement of an appointment

WiTCOM will arrange an appointment of the service technician with the customer in so far as required.

This appointment will be indicated as a time span not exceeding two hours (e.g. “between 10 a.m. and 12 a.m.”).

If the service cannot be provided within the agreed period of time for reasons which lie in the responsibility of the customer, a new appointment will be arranged, and, if necessary, an additionally required journey will be charged for.

5.9 Other fault reporting

In so far as the customer is liable for the failure (caused in or by customer facilities, or falsely reported fault information by the customer), WiTCOM shall be entitled to claim compensation for the expenditure incurred.

This case will be treated as an “additional service” and charged for on a time and materials basis;

The hourly rate for a system technician (installation and configuration of actively used technology as well as fault clearance works for which a third party is responsible, as well as project control) is given in the WiTCOM hourly rates price list.

6. TERMS OF CONTRACT

The General Terms and Conditions of business of WiTCOM GmbH (GTC) shall apply. In the event of deviations, the regulations of this statement of work shall have priority over those stipulated in the GTC.

6.1 Contract term

The minimum contract term for WiTCOM MPLS VPN is 12 months and will be individually agreed with the customer.

For further details such as notices of termination please refer to section 18 WiTCOM GTC.

6.2 Terms of payment

The customer shall pay to WiTCOM the charges due for the transfer of WiTCOM MPLS VPN. These charges include the billing items “one-time provision charges” and “monthly charges”.

For the service changes “upgrade”, “downgrade”, or any circuit switchover (including moving within the same building) WiTCOM will charge the difference between the one-time provision charges of the previous and the new WiTCOM MPLS VPN, however, not less than 50% of the provision charges valid for the new WiTCOM MPLS VPN.

7. LIABILITY

The network termination unit remains WiTCOM property. Upon contract termination the network termination shall be returned to WiTCOM in its initial configuration. The customer shall be liable for damages to the network termination caused by the customer or by third parties which are under its sphere of responsibility.