

SERVICE DESCRIPTION FOR EQUANT INTERNET VPN

1. **Definitions.** All capitalized terms used but not defined herein will have the meaning given to such terms elsewhere in the Agreement. In the event of any conflict between the definitions provided in this Service Description and those provided elsewhere in the Agreement, the definitions in this Service Description will control for purposes of this Service Description.

“**Encryption Equipment**” means the hardware and software provided by Equant for the Internet VPN Service that enables the IPSec protocol.

“**IP**” or “**Internet Protocol**” means a part of the TCP/IP family of telecommunications protocols describing software that tracks the Internet address of nodes, routes outgoing messages and recognizes incoming messages.

“**IPSec**” means “**IP Security**”, which is a protocol that enables secure end-to-end sessions to be established over a public network (e.g., the Internet).

“**ISP**” or “**Internet Service Provider**” means a third-party that provides Customer with access to the Internet.

“**Node**” means a node of the Equant Network to which Customer is connected via a Tail Circuit or to which Customer dials in, such Nodes being deployed at such times and places as determined by Equant.

“**VPN**” or “**Virtual Private Network**” means a private network that is configured within a larger network.

2. **Service Overview.** The Equant Internet VPN Service is a managed branch-to-branch VPN service that employs the Internet as a transport mechanism for IP traffic and uses an IPSec security layer, connecting Locations in a hub and spoke topology. The Internet VPN Service is recommended for the transmission of data that is non-mission critical, or **not** delay-sensitive. The Internet VPN Service is provided via: (i) the Equant Internet Direct Service, as described in a Service Description attached to this Agreement (“**On-Net**”), or (ii) Internet access provided to Customer by an ISP (“**Off-Net**”).

3. **Customer Certification.** Customer hereby certifies that it will not relocate the Encryption Equipment from the Locations specified in the Order(s) and that it is not acquiring the Encryption Products for stocking purposes.

4. **Internet VPN Connection.** Equant provides a LAN-to-LAN (Local Area Network-to-Local Area Network) interconnection, which enables (through an end-to-end IPSec tunnel) transmission of Customer’s IP traffic to other Locations within the VPN. The Internet VPN Service includes:

- Either On-Net or Off-Net access, as selected by Customer;
- Design and configuration of the Internet VPN;
- Provisioning, configuration and maintenance of the CPE; and
- Provisioning of end-to-end IPSec tunnels between Locations.

For On-Net configurations, the Internet VPN Service also includes:

- The requested IP bandwidth for the Location;
- Regular reporting on the Internet VPN Service performance

(i.e., Quality of Service indicators); and

- Provisioning and monitoring of the access leased line connecting a Location to the Equant point of presence.

5. **Access Methods.** For On-Net configurations, access methods include native IP leased lines, Equant Frame Relay, Equant ATM, Equant DSL in countries where DSL access is available, and fiber into an Equant Internet Direct Node. For Off-Net configurations, the Internet VPN Service will be provided over Internet access provided to Customer by an ISP.

5.1 **On-Net Access via the Equant Network.** For all On-Net configurations, Customer must connect into an Equant Internet Direct Service Node. Dedicated access is supplied through a Tail Circuit, in which the requested IP bandwidth is configured for Customer based upon the Location’s requirements. Customer will select the applicable bandwidth, and Equant will determine the access method. Equant will upgrade the IP bandwidth upon Customer’s request, provided that the IP bandwidth parameter will not exceed the Tail Circuit bandwidth.

Each Location will be able to communicate with other VPN Locations (either hub or spoke) based on the Internet VPN Service routes defined by Customer, which routes will define the configuration of the IPSec tunnels.

5.2 **Off-Net Access via ISP.** For Off-Net configurations, Customer will subscribe directly to an ISP service, and Equant is not responsible for providing the Internet connectivity. The supported Off-Net access methods are:

- Dedicated access through a leased line to an Internet point of presence; or
- Broadband access via ADSL or a cable modem, using an Ethernet connection.

The ISP must provide an Ethernet interface, to which the Equant CPE will be connected. Customer will provide Equant with the accurate IP address of the WAN (Wide Area Network) interface provided by the ISP, which address is required for Equant to configure the CPE router.

6. **Managed CPE.** For both On-Net and Off-Net Internet VPN Service, Equant will provide managed CPE, including all router hardware and Software as well as the maintenance for such hardware and Software, as more fully described in the Service Description for LAN Access attached to this Agreement.

7. **Equant IPSec Security Elements.** The IPSec protocol will be activated at the CPE level to perform the following functions: (i) encryption; (ii) tunneling; (iii) authentication; and (iv) Integrity checking.

8. **Acceptance Testing.** The Internet VPN Service will be deemed operational when the CPE router is able to send and receive IP traffic to other VPN Locations using the IPSec tunnels configured with other Locations. Equant will perform a basic connectivity test to check the end-to-end connectivity. This test will consist of an extended ping to the private interface of the remote CPE router.

9. **Service Reporting.** Customer may access reports for the Internet VPN Service via the WebVision Service, which is described in a separate Service Description attached to this Agreement.

END OF SERVICE DESCRIPTION FOR INTERNET VPN SERVICE