SPRINT GLOBAL MPLS VPN
PRODUCT ANNEX

The following terms and conditions, together with the Sprint Master Services Agreement, Custom Service Agreement or other Sprint agreement ("Agreement") and the Sprint Standard Terms and Conditions for Communication Services ("Standard Terms and Conditions") will govern Sprint's provision and Customer's use of the Sprint Global MPLS VPN Service (the "Services") specified in the applicable order form ("Order").

1. Services Description. Sprint's Multiprotocol Label Switching Virtual Private Network ("MPLS VPN") solution is a network-based IP VPN available globally across Sprint's IP/MPLS backbone. This solution provides customers with a secure IP VPN solution with any-to-any intranet connectivity and a private means by which to connect their enterprise sites. In addition, customers can purchase Value Added Services ("VAS"), such as Secure Internet Access with Network-based Firewall, all on the same underlying network infrastructure.

2. Order Term. The initial Order Term for the Services will be stated on the Order and will begin on the first day of the billing month following the date Services are installed and available to Customer. At the end of the initial Order Term, the term will renew on a month-to-month basis. Either party may terminate the Order at the end of the initial term or during a renewal term by providing the other party 30 days' prior written notice.

3. Primary Service Components. The primary service components for the Services are as follows:

3.1. Global MPLS VPN Port(s). A Port is the physical entrance to the Sprint network.

A. Port Charges. Sprint will charge Customer a Non-Recurring Charge ("NRC") and a monthly charge for each Services Port, including all sub-elements or configurable attributes to the Port. The Network Design Document and Port Order will specify the sub-elements or configurable attributes to the Port (e.g. Port speed, link protocol, routing protocol, VRF policy, Class of Service (for DS3/E3 and below), and where Customer requests, Multicast VPN). For monthly charges, Sprint offers both fixed rate (Monthly Recurring Charge or "MRC") and usage-based (Burstable) Port pricing. For Burstable Port pricing, Sprint will provide Customer with a full Port at a given bandwidth and will charge Customer a variable monthly charge based on Customer's sustained Port utilization. Sprint will determine Customer's Port utilization and charges at the end of each month. Additional information regarding Sprint's Port utilization computation is available upon request.

B. Port Upgrades. Customer may upgrade an existing Port before an Order Term expires without incurring early termination liabilities for that Port, if the upgraded Port: (1) is installed at the same location as the replaced Port; (2) is installed within 10 days after the replaced Port is disconnected; (3) has an Order Term equal to or greater than the remaining Order Term of

the replaced Port, subject to a one year minimum; and (4) has greater Port bandwidth than the replaced Port.

C. Additional Port Terms and Conditions. Ports are subject to availability of capacity. If Customer's Port resides in a Sprint Shared Tenant facility, Customer is responsible for working with the site vendor to order the cross connect and will be invoiced by the site vendor for any fees associated with the cross-connect.

3.2. Digital Signature Client Software. This software is used to encrypt email communication between Customer and Sprint regarding service requests. Sprint will provide Customer digital certificates and digital signature client software licenses for 2 Customer points of contact at no charge. If Customer requires more than 2 software licenses, Customer may purchase additional licenses from Sprint at Sprint's then-current list rate. If Customer purchases Sprint Managed Network Services, Customer will receive 2 additional licenses at no charge.

4. Additional Required Components. The Services also require Customer to have the following:

4.1. Dedicated Local Access. Dedicated local access is required for the Services. Customer may purchase Sprint-provided local access facilities, which will be provided under separate agreement with Sprint, or Customer may provide its own local access facilities.

4.2. Customer Premise Equipment ("CPE"). CPE is required for the Services. Customer may elect to purchase CPE from Sprint or provide its own CPE. CPE includes, but is not limited to the following:

A. Routers. Unless Customer has separately contracted with Sprint to provide additional support services, Customer is fully responsible for the router, including configuration, maintenance, and management. In addition, if Customer elects not to obtain a router from Sprint, Customer must furnish the necessary ancillary equipment (cables, routing software, etc.) to ensure interoperability with the Services.

5. MPLS over Digital Subscriber Line ("DSL"). Customer sites may qualify for alternate access via MPLS DSL. This eliminates the need for a MPLS Port and access at the qualifying site. MPLS DSL sites may communicate freely with other MPLS DSL and MPLS locations. Customer must have at least one MPLS Port in its network.

6. Value-added Services. Sprint provides Value-added Services ("VAS") that Customer may opt to purchase as part of its Global MPLS VPN solution. VAS have both a monthly charge and an NRC. For monthly charges, Sprint offers both fixed rate and variable (usage-based) VAS pricing. For usage-based VAS pricing, the monthly charge will vary based on the aggregate bandwidth Customer utilizes each month. Customer must select either fixed rate or usage-based pricing for its entire network.

6.1. The following VAS are Network-based:

A. Secure Internet Access ("SIA") with Network-based Firewall. Regional VAS gateways provide secure access from the Services to the

Internet. Each site in Customer's Global MPLS VPN will receive Internet access secured by a stateful inspection firewall located within Sprint's network.

B. Remote Access Service ("RAS"). RAS allows Customer's employees or users to obtain remote access to the Services through the use of a VPN client. This client is installed on an employee's or user's laptop and builds an IPSec tunnel back to a VAS gateway to enable employees or users to run corporate applications while away from the office.

6.2 IPSec Half Tunnel. Internet Protocol Security ("IPSec") Half Tunnel is for customers who have sites outside Sprint's footprint or have the need to securely communicate with a select audience outside of their organization. IPSec Half Tunnel allows Customer to connect to the Services using Sprint's Managed CPE-based IP VPN, which can be used at locations where Customer has existing dedicated internet access from Sprint or from another service provider. Alternatively, Customer or a third party can elect to manage the CPE-based IP VPN device. In a Sprint-managed solution, Sprint will design, implement, maintain, and manage hardware at CPE-based IP VPN locations, providing a complete end-to-end VPN solution.

7. Invoicing. MRCs are billed in advance for all services provided during the following billing period. The first and last invoices will include prorated MRCs based on the first and last day of service. The usage-based charges above and beyond MRCs are billed in arrears.

8. Customer Responsibilities

8.1. Multicast VPN

A. If Customer requests Multicast VPN, the following are Customer's responsibilities:

(1) Customer must run its own rendezvous points (depending on the protocol it is using) and servers. Sprint does not provide (or have) rendezvous points for Multicast VPNs. The Sprint network is essentially invisible to Customer.

(2) Customer must provide its own Multicast addresses. Sprint makes no restrictions on addresses, but Multicast is limited to the Class D range (224.0.0.0 - 239.255.255.255).

(3) Except for verifying that Multicast traffic is coming in on one router and exiting on the other side, Customer must manage Multicast. In other words, Sprint will verify that Multicast traffic is coming from Customer and that Sprint is sending Multicast to Customer on the other side. Sprint will not be able to access Customer's Multicast transmissions and will not be able to verify that the transmissions are successfully working. After implementation, Sprint will troubleshoot and add data addresses if Customer's need for Multicast groups grows.

8.2. IPSec Half Tunnels

A. If Customer elects to manage the CPE-based IP VPN device, the following are Customer's responsibilities:

(1) Customer must coordinate communication between Sprint and any third parties involved in managing Customer's network or with the partner who is using the Half Tunnel connection.

(2) Customer must participate and support the service delivery objectives in the provisioning of the Half Tunnels and any associated transport orders.

(3) Customer must monitor Customer-managed IP VPN devices.

(4) Customer is responsible for repairing any issues or outages with Customer-managed devices.

9. Network Monitoring

9.1. As part of the Services, Sprint provides Customer a trouble resolution team available to respond to Customer's issues 24 hours a day, 365 days a year. Customer may elect to purchase additional monitoring and management services as described in Section 10 below.

9.2. Sprint will provide a trouble ticket number from Sprint's automated Trouble Reporting System ("TRS") to Customer's help desk that reports the trouble. For each trouble report, TRS will maintain information about the trouble, the steps taken to resolve the trouble, and the final disposition of the trouble report. Sprint will keep Customer's representatives apprised of the status of service restoration actions.

10. Enhanced Monitoring and Managed Services. For customers interested in purchasing enhanced monitoring and managed services for the Services, Sprint offers the following:

10.1 Managed Network Services. These services include a comprehensive suite of management and implementation services that support multi-protocol Wide Area Networks (WANs) and Local Area Networks (LANs) utilizing Sprint and non-Sprint provided transport services. These services support customer premises-based routers, IP-VPN devices, switches, hubs, servers, and applications worldwide. Sprint Managed Network Services is comprised of engineering, design, and implementation of customer networks, including WAN transport; LANs and CPE; day-to-day operational support; configuration management; network and CPE monitoring; proactive notification; fault management; trouble resolution; and network and device performance reporting.

10.2 Sprint E-mail Protection Services. These services provide inbound and outbound content blocking, policy management, anti-virus and spam management (including message quarantine service), disaster recovery, outbound anti-virus management and SMTP Services, web reports, and web administration.

10.3 Managed Security Services. These services include a comprehensive suite of management and implementation services that support security related

functionality. The services support firewall, intrusion detection and prevention services, DDOS detection and mitigation, and URL and content filtering. Customer entitlements include engineering; design and implementation of services; day-to-day operational support; configuration management; security event monitoring; proactive notification; fault management; trouble resolution; and network and security event reporting.

11. Service Level Agreement. All applicable Service Level Agreements, as Sprint may amend them from time to time, will apply during the Order Term.