SPRINT MANAGED SECURITY SERVICES
PRODUCT ANNEX

The following terms and conditions, together with the Sprint Master or Custom Services Agreement or Domestic Sprint Services Sales Application Form ("Agreement"), will govern Sprint's provision and Customer's use of Sprint Managed Security Services ("Services") as specified in the applicable order form or Statement of Work ("Order"). If a conflict exists between the Agreement and these terms and conditions, these terms and conditions will control.

1. **Term.** The initial term for the Services ("Initial Term") will be stated on the Order or will begin on the first day of the month following the date the Services are installed and available to Customer, whichever is later ("Service Availability Date"). Invoicing for Services will begin on the Service Availability Date. UPON THE EXPIRATION OF THE INITIAL TERM, THE ORDER WILL BE AUTOMATICALLY EXTENDED FOR SUCCESSIVE ONE MONTH PERIODS, UNLESS EITHER (A) CUSTOMER OR SPRINT PROVIDES 30 DAYS' ADVANCE WRITTEN NOTICE TO THE OTHER THAT IT WISHES TO TERMINATE THE ORDER, OR (B) THE PARTIES EXECUTE A NEW ORDER FOR SUCH SERVICES WITH A MINIMUM TERM OF ONE YEAR.

2. **Prices.** Prices will be stated on each Order. Prices are fixed for the Initial Term. Thereafter, Sprint will provide Customer with written notice of any price changes at least 30 days prior to the effective date of such changes. In the event of such changes, Customer may terminate the Order without termination liability by providing written notice to Sprint no later than 30 days prior to the effective date of such changes, otherwise Customer will be billed according to the new prices and/or discounts beginning on the effective date of such changes.

3. **Delivery of Customer Premise Equipment.** If Services include Customer Premise Equipment, Sprint will schedule the delivery of the Services in accordance with the mutually agreed delivery date specified in the Order. Sprint will accommodate one Customer-requested delay in the delivery date specified in the Order, provided that: (a) such delay does not exceed 30 calendar days from the delivery date specified in the Order, (b) Sprint receives such Customer requested delay in writing no later than 10 days prior to the original delivery date, and (c) Customer agrees to pay any additional charges resulting from such delay. If Customer delays delivery of the Services for more than 30 calendar days beyond the delivery date specified in the Order, then Sprint will invoice Customer for all Services charges effective 30 calendar days from the original agreed delivery date. Customer-delayed Orders cancelled more than 30 days after the delivery date specified in the Order are subject to Sprint's cancellation charges, which consist of the following: (a) a re-stocking charge equal to 10% of the purchase price of the hardware and software which is applicable to either the rental or purchase of equipment, (b) any termination charges incurred by Sprint from its third-party service providers, and (c) any travel and living expenses incurred by Sprint and direct labor costs associated with any effort by Sprint with respect to the canceled Order.

4. **License Use**. Sprint-provided software may only be used on a single computer located in the United States and its territories or any other country to which the software may be legally exported.

5. **Service Components**

5.1 Sprint Managed Security Services is made up of the following products or services: firewalls, intrusion detection/prevention systems, web content filtering, distributed denial of service detection and protection, and user authentication services, unified threat management, secure log management and compliance, vulnerability monitoring, pci dss scanning and assessments, and hosted anti-virus. Within each of these services are several components that comprise the offering described below. These components may not be applicable to all services.

A. Security Design. Sprint will work with Customer to create a Security Engineering Design Document ("SEDD") for each security device within the network, describing the configuration and accompanying service levels that meet Customer's established security policy. This design is developed to minimize Customer's risks associated with threats and vulnerabilities. Sprint reserves the right to modify the SEDD in response to additional information on Customer's needs.

B. Implementation. Implementation is the process by which all equipment is tested, software burned in, Customer-specific data loaded, and equipment inventory checked for accuracy. This process helps to ensure dependability of the equipment and minimized onsite installation time. Implementation may be completed by Sprint, the vendor, or a third-party partner, depending on location or product purchased.

C. Installation. Sprint provides security device installation to all customers (Sprint-managed and customer-managed). Installation may be provided by Sprint, the vendor, a third-party partner, or any combination of these providers, depending on location and product purchased.

D. Hardware and Software. Hardware and software includes the equipment and software needed to implement the security solution that was designed. Customers may rent or purchase hardware and/or software from Sprint for United States locations. At this time, export restrictions apply on devices for global locations.

E. Management and Monitoring. Management and monitoring are real-time service provided by Sprint's Secure Network Operations Centers (SNOC). Services include: 24 hours per day, seven days per week ("7 x 24 x 365") proactive monitoring, change request support, network management, configuration management, customer reporting and alert notifications as deemed necessary. Depending on the product, different levels of management may be offered.

F. Hardware Maintenance. Hardware maintenance provides for the repair or replacement of device hardware in the event of hardware failure. Depending on the device and country, maintenance services may be provided by Sprint, the hardware vendor, or a third party. Maintenance service options also vary by device and country.

G. Software Maintenance. Software maintenance is also required for some of the products, providing revision level upgrades, patches, bug fixes and anomaly support.

H. Shipping - Non-U.S. Locations. For locations outside the continental U.S., additional shipping services and fees are required to address the added freight, duty and customs expenses involved with shipment of devices. Export restrictions may also apply.

6. Responsibilities of Sprint

6.1 Sprint will design, implement, install, manage and monitor the Services as required in the Order.

6.2 Sprint warrants that Services will be in good working order and will conform to the requirements of the Order in effect on the date Services are available to Customer. Customer's sole remedy for non-performance of Services will be repair or replacement of the Services by Sprint at no additional charge to Customer.

6.3 The Services are designed to assist in enforcing customer's security policies and deterring unauthorized access of Customer's telecommunication network. Sprint's sole responsibility is to provide and, at Customer's option, manage such Services according to the level of management selected by Customer in the Order. The Services may not completely eliminate unauthorized network access and the resulting charges. Sprint is not responsible for any unauthorized access to Customer's network and any telecommunication charges incurred by Customer as a result.

7. Customer Requirements

7.1 Managed customers must adhere to the following requirements:

A. Sprint must design the Services to ensure all the managed security devices are properly integrated into Customer's network and overall security infrastructure.

B. Managed customers must supply a standard phone line at each managed security device location that can be connected to an encrypting modem for remote support by Sprint.

C. Only Sprint can have access to the configurations of all security devices comprising the network. This level of control assures that Sprint is the only entity able to make changes, and ensures configurations between devices will provide consistently functional connectivity.

8. Secure Web Portal Access

The Sprint SNOC utilizes a secure web portal to communicate all Customer information. Customer will be provided a web (SSL) user ID and password to authenticate with the web portal. For enhanced security, Customer may choose to utilize digital certificates to authenticate and encrypt all communications. Customer will be charged a one-time fee for each digital certificate.

9. Security Devices

9.1 Administration. Sprint will administer managed security devices 7 x 24 x 365. Day-to-day administration occurs through the processing of change request forms. Sprint accepts and processes these forms 7 x 24 x 365. Customers can submit these change requests and inquiries via the secure online web portal.

9.2 Out-of-Band Firewall Access for Security Device. Sprint will provide an encrypting modem attached to the security device when at Customer's premise as an alternate method of communicating with the managed security device, in the event that the primary transport is not available. Customer is responsible for providing a dedicated voice circuit for connection to the encrypting modem when the managed security device is located at Customer's premise.

9.3 Security Device Management and Monitoring.

A. Sprint will provide 7 x 24 x 365 monitoring of Customer's security device for hardware and software problems. When a problem is identified, Sprint will notify Customer according to the method of notification agreed upon in the SEDD. Communication vehicles include electronic mail, telephone, fax, and pager. Sprint will notify only the Customer-designated points-of-contact defined in the SEDD. If Sprint is unable to reach the points-of-contact for any reason, a voice-mail followed by electronic mail will serve as default notification.

B. Customer is responsible for ensuring Sprint has up-to-date information on all points-of-contact. Sprint is not responsible for unsuccessful notifications due to out-dated point-of-contact information.

9.4 Security Device Hardware and Software Upgrade Procedures

A. Hardware Upgrades. Sprint will provide pro-active performance management. Sprint will track and analyze firewall performance statistics to ensure that Customer's security device hardware is properly sized. When Sprint determines that security device performance is degrading, Sprint will recommend appropriate action. In addition, if Customer security device moves to end of life status as determined by the equipment vendor, Customer will be migrated or upgraded to a new security device within 90 days of end of life determination. Customer will be responsible for any and all charges incurred to upgrade the hardware, including installation.

B. Software Upgrades

(1) Sprint tests, validates, and certifies all major security device software releases before installing them. Sprint has the following policies regarding security device software installations and upgrades:

(a) Sprint reserves the right to upgrade Customer's security device software revision level if the installed revision level is no longer supported by the security device vendor.

(b) Sprint reserves the right to upgrade Customer's security device software to fix software bugs in the existing version.

(c) When adding new security devices to Customer's existing network, Sprint reserves the right to install the same version of the security device software running on an existing security device onto the new security devices rather than upgrade the entire network with the latest software release.

(d) Sprint will not be required to install the latest revision until it is tested and validated by Sprint and the parties agree there is a business need or the current version of the software being used is no longer supported by Sprint.

(2) Some major software upgrades will incur upgrade charges (determined by vendor). No changes incurring additional charges will be made without Customer's approval. If Customer refuses to allow Sprint to make a Sprint-recommended upgrade, Sprint will not take responsibility for the performance or security of the security device.

(3) Sprint will install all operating system security patches deemed necessary to ensure the security of the underlying system.

9.5 Software updates will be performed remotely by Sprint personnel during the maintenance window defined in the SEDD and with Customer coordination if deemed necessary.

9.6 Security Device Hardware Failure. During business hours, if Sprint determines that hardware has failed, Sprint will contact Customer's point-of-contacts and, if necessary, dispatch an engineer to the affected site according to the service level agreement. In the event that a failure occurs during non-business hours, Customer's point-of-contact will direct Sprint as to when an engineer can gain access to Customer's facilities.

9.7 Security Device Reporting and Normalized Logs. Sprint will make security device usage reports and normalized log files available for Customer access via a secure website. These reports/ will be available by the 10th business day of each month. These reports and raw logs will be available online for 90 days and then archived to tape and stored off-site for up to 36 months or term of the customer contract, which ever is more.

9.8 Security Device Backups. Sprint performs nightly backups of Customer's security device configuration files. These backups are stored online for 60 days and then archived to tape and stored off-site for up to 1 year. These configuration files are readily available if a rebuild of the firewall is necessary. The backups take place between midnight and 6:00 AM ET.

9.9 Change Control

(1) Customer and Sprint must follow strict change control procedures to ensure the performance and security of a security device. All changes initiated by Sprint require Customer's approval before implementation.

(2) Firewall access components are rules, applications, systems, users, and groups. Only the designated Customer point-of-contacts will be permitted to request changes to the firewall access components. Sprint will accept change request forms through a digitally signed electronic mail message or via a submission onto the secure customer web portal. Sprint will track all changes made by Sprint personnel on the managed security device. When a change is made, Sprint notes the existing change configuration, records any changes, explains why a change was necessary, and records any relevant authorization information.

(3) Customer will classify all changes as emergency, simple, complex or redesign on the change request form. There are monthly limitations to the number of changes that will be made as a part of the management level in Customer's Order. If Customer exceeds the maximum allotted monthly changes, based on the management level, the Overage Charges shown in Customer's Order apply to each subsequent request. Each request submission is calculated separately.

(4) The Sprint SNOC will acknowledge all new change requests and provide a response to the requestor within 4 hours of submittal. A simple change request will be completed within 24 hours of submittal. A complex change request will be completed within 72 hours of submittal. Simple and complex change requests submitted for multiple devices will be completed on a best effort basis, which will be communicated to the customer during the processing of the change request.

(5) Customer can submit a change request to be completed outside the mentioned windows for simple or complex change requests. A 2-hour window must be provided for these changes, during which time Sprint will process the change. Sprint will process this change at any point during this window, unless specifically requested by the customer for a particular timeframe and confirmed by a Sprint engineer.

(6) Customer can submit an emergency change request to be completed within (4) hours. Once the emergency request is submitted via the secure web portal, Customer should immediately contact the Sprint SNOC Network Change Request team at 1-877-368-7915 or 703-464-2909 for international callers. The emergency change request allows the Sprint SNOC to shut down parts or all of Customer's network without prior notice, in order to complete the request.

(7) If a network redesign is required, Sprint will charge a fee to Customer (one-day, on-site consulting) to review the entire design with Customer. A redesign may be required by the following:

(a) the network backbone is increased or decreased by more than 50%;

(b) Customer requests firewall rule changes that result in over 50% of the rules or user accounts on the firewall needing modification and exceeds the maximum number of changes allowed within the time period; or

(c) Customer switches the hardware platform or firewall architecture for another.

(d) The change request contains information that is "out of scope" of standard daily operations (e.g. half tunnels that require additional resources in order to complete the request).

9.10 Scheduled Maintenance Procedures. From time to time, Sprint will need to perform software and hardware maintenance on Customer's security systems. All maintenance will be scheduled by Sprint and performed during Customer's maintenance window, which will be defined in the SEED. Sprint will notify Customer's point-of-contact during normal business hours of any necessary maintenance down-time. For any maintenance that requires on-site personnel, Sprint will arrange an appropriate time and necessary premise access.

9.11 Service Disconnects. If Customer requests to discontinue the security device or service, Customer will be required to pay a recovery fee (one-day, on-site consulting) for Sprint to go to Customer's site and recover the security device hardware and software. If the hardware is damaged, Customer will pay up to the then-current list price (fair market replacement value) for the hardware components.

9.12 Managed Security Services Charges. If Customer submits emergency change requests, exceeds the maximum allotted number of simple or complex monthly changes or submits a redesign request the Service Charges as shown in the tables below apply to each subsequent request. Each request submission is calculated separately.

MANAGED SECURITY SERVICE OVERAGE CHARGES

Type of Change	**Change Management Guarantee**	**Max Changes/ year**	**Service Charges** When the yearly allotted changes are exceeded, the following charges apply to each subsequent request
Simple Change Request	All validated, non-bulk simple change requests will be implemented within 24 hours of receipt. Bulk changes (more than 50 changes submitted together) should be scheduled with the MDS NCR Team	120	$75 per simple change request submission
Complex Change Request	All validated complex change requests will be implemented within 72 hours of submittal. Bulk changes (more than 50 changes submitted together) should be scheduled with the MDS NCR Team	0	$200 per complex change request submission
Redesign Request	Redesign requests will be completed within a timeframe dependent on the complexity and length of the change. If a change request is designated as a redesign, the Sprint account team will contact the customer in order to coordinate the change. All new features or requests on the current service will be classified as a Redesign.	0	$200 per hour or pricing determined on individual case basis (ICB)
Emergency Request	All validated emergency change requests will be implemented within four hours from the receipt of the request. These change requests (regardless of size) will be processed immediately, however, a maximum of 2 emergency changes are guaranteed to be completed per hour.	0	Billable per request. Pricing determined on individual case basis (ICB)