SprintSecure^{sm} Message Protection Product Annex

The following terms and conditions in this **SprintSecure**^{sm} Message Protection Product Annex ("Annex"), together with the Sprint Standard Terms and Conditions for Communications Services or Sprint Master or Custom Services Agreement or Domestic Sprint Services Sales Application Form ("Agreement"), as applicable, will govern Sprint's provision and Customer's use of Sprint Message Protection services as specified in the applicable order form or Statement of Work ("Order").

1. DEFINITIONS.

1.1 "Customer" shall be defined herein as it is defined in the Agreement.

1.2 "Domain Name Host" is the in-house or external organization or entity that is providing the Customer with DNS services for the Customer**'**s domains.

1.3 "Domain Name Server" shall mean a server which implements the Domain Name System (DNS) that defines procedures for referrals to other name servers and for the use of domain names in the delivery and retrieval of SMTP email on the Internet. The domain name system also defines procedures for caching retrieved IP mappings and for periodic refreshing of these mappings by domain name administrators.

1.4 "Downtime" is defined as any time during which Sprint fails to provide any of the Services, measured from the time of actual interruption of the Services, until the time such Services are restored.

1.5 "Minimum Monthly Recurring Commitment" shall be defined as the minimum amount to be billed by Sprint to Customer regardless of Customer's actual Throughput or number of Seats.

1.6 "MX Record" shall mean a "mail exchanger" record, which is the resource record used in the domain name system that allows the mapping of a hostname to its mail server.

1.7 "Seat" shall be defined as a recipient on behalf of which e-mail messages are being sent (i) from Customer's network(s) or server(s) to the Sprint network or (ii) through the Sprint network for delivery to Customer's network(s) or server(s).

1.8 "Service Credit" shall be defined as the percentage of the monthly pro-rated service cost of the Services that is awarded to Customer for a validated claim. The service credit percentage awarded may vary with each SLA and will depend on the estimation of service performance.

1.9 "Services" shall be defined as those message filtering, message archive, message continuity and message encryption services included in the service package subscribed to by Customer as set forth in the Agreement and/or the Order.

1.10 "Sprint Network" shall mean the network of data centers, data connections and services that Sprint maintains to provide services to Customers.

1.11 "Throughput" is defined herein as the total amount of all messages processed by Sprint pursuant to the Agreement that are addressed to the Customer or originate from the Customer's email server, measured in megabytes on a monthly basis.

2. RESPONSIBILITIES OF CUSTOMER.

2.1 It is understood that the Services shall not include Customer's access connection to the Internet or any equipment necessary for Customer to make such connection, which shall be the sole responsibility of Customer.

2.2 Customer is responsible for establishing and maintaining a suitable Domain Name Server either directly in-house or through a third party Domain Name Host.

2.3 Customer is responsible for notifying its Domain Name Host, if any, that Customer's inbound email shall be re-directed to Sprint and Customer is also responsible for causing any and all required changes to Customer's MX record and, where applicable, to the outgoing mail on the Customer's mail server, to facilitate such redirection.

2.4 Customer's use of the Services is subject to all applicable local, state, national and foreign laws and regulations. Customer agrees to comply with such laws and regulations and with Sprint's most current AUP.

2.5 Customer is solely responsible for the contents of any and all e-mails originating from Customer.

2.6 Customer is solely responsible for its activities in using the Services including the activities of its employees and its contractors and all parties that Customer allows to have access to the Services provided by Sprint.

2.7 Customer must maintain a valid IP address to enable Sprint to provide the Message Protection service to Customer. Sprint shall not be responsible for the inability to provide such service to Customer if Customer's IP address is not valid.

2.8 If Customer is charged fees on a per seat basis, Customer must notify Sprint if the number of Customer's seats increases by more than 5% of the then declared number of seats.

2.9 If Customer is charged fees on a flat fee per month basis, the fee is subject to renegotiation if the number of Customer's seats or Customer's expected Throughput volume increases by more than 5% than the declared number of seats or estimated Throughput volume included in the Order.

2.10 Customer agrees to monitor all uses of its account, notify Sprint of any unauthorized use of Customer's account, and set up IP restrictions per the Sprint guidelines to protect SMTP services.

2.11 A list of all Customer domains that are to be covered by Supplier Services (e.g. yourdomain.com) will be determined by the Customer and Sprint before initial commencement of Services. Domains not identified will not be covered until the Service begins. The email server name will be determined by Sprint and Customer at a later date.

3. RESPONSIBILITIES OF SPRINT.

3.1 Sprint shall take commercially reasonable security measures to protect the confidentiality of Customer's email. Further, Sprint shall not monitor, censor or edit the contents of Customer's email messages, unless required to do so by law or in a good faith belief that such action is necessary to protect the safety of the public, Customer or Sprint. In the event that Sprint becomes legally compelled to disclose any of Customer's email, it shall provide prompt, prior written notice of such requirement to Customer so that Customer may seek a protective order or other remedy. For the sole purpose of performing the Services and without reviewing any substantive content pertinent to Customer, Sprint may track, view and manage email messages which it has good reason to believe are spam or are contaminated by viruses.

3.2 Sprint reserves the right to suspend Services to Customer if Customer's server(s) is used as an open relay that allows third parties to relay e-mail messages through Customer's server(s) to other recipients. In such a case, Sprint will use its commercially reasonable efforts to promptly contact Customer and give Customer the opportunity to promptly change the configuration of its server(s) to avoid the use of Customer's server(s) as an open relay.

3.3 Sprint represents and warrants that it has and shall maintain all rights, licenses and permits necessary and required by law to provide the Services to Customer. Sprint grants to Customer the necessary licenses to use the Services.

3.4 Sprint shall not be responsible for backing-up or archiving Customer's email after delivery to Customer's designated email server and Sprint assumes no responsibility for the operation of Customer's network or servers or any deletion or failure to store email messages after delivery of the same to Customer.

4. SERVICE LEVEL AGREEMENT.

4.1 SLA Claims

4.1.1 Sprint provides these SLAs and related terms to Customer subject to the following terms, which may be updated by Sprint in its sole discretion from time to time without notice to Customer. Customer can review the most current version of the SLAs and related terms at any time by visiting http://admin.global.sprint.com and clicking the Resource Center link.

4.1.2 If Customer believes that Sprint has failed to meet its SLA commitments under any of the below SLAs, Customer must contact Sprint Customer Support in a timely manner in writing within 5 business days from the date of the incident in which Customer believes the SLA obligations were not maintained. In the event it is clearly shown that Sprint did not meet its SLA commitments, Sprint's sole obligation to Customer will be to provide a credit to Customer against future service fees in an amount equal to the Customer's monthly Service charge for the month during which the commitments were not maintained multiplied by: (i) the number of days during which Sprint failed to meet its commitments in the month, divided by (ii) the total number of days in that month;

4.1.2.1 For all claims subject to validation by Sprint. Sprint will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment (in Sprint's sole discretion) on the applicability of SLAs to said incident;

4.1.2.2 In the event that more than one aspect of the service is affected by the same root cause, the single SLA of Customer's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.

4.1.2.3 These SLAs do not apply

- To trial customers or trial domains
- During the first thirty (30) calendar days of service for newly subscribing or implementing customers

4.2 Configuration Requirements

4.2.1 Customer must adhere to the required configurations of the best practices guide, available for download from the Admin Center Resource Center, to make claims against SLAs;

4.2.2 Customer must not act as open relays, open proxies, or send any form of bulk, unsolicited email, or any other activity deemed in violation of applicable terms of use of Acceptable Use policies.

4.3 Remedy

4.3.1 The remedies outlined in this document are Customer's sole and exclusive financial remedies

4.3.2 The remedies awarded in any calendar month shall not, under any circumstance, exceed the monthly service fees based on the number of licenses purchased.

5. Message Filtering Network Uptime SLA - 99.999%
Definition: The percentage of time in a calendar month that the network is able to receive and process email messages.

5.1 Includes emergency and planned maintenance

5.2 Remedy – see table:

Message Filtering Network Uptime SLA	
% of Service Availability per Calendar Month	**Service Credit**
< 99.999%	25%
< 99.0%	50%
< 98.0%	100%

6. Message Filtering Email Delivery - < 2 minutes
Definition: The average of email delivery times, measured in minutes over a calendar month, where email delivery is defined as the elapsed time from when a business email enters the Message Filtering network to when it exits the network.

6.1 Email delivery time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month.

6.2 Sprint may use simulated or test emails to measure delivery time

6.3 Applies only to legitimate business email (non-bulk email) delivered to valid email accounts
6.4 This SLA shall not apply to:
6.4.1 Delivery of email to quarantine
6.4.2 Email in deferral queues

6.4.3 Denial of Service attacks (DoS)
6.4.4 Email loops

6.5 Remedy – see table:

Message Filtering Latency SLA	
Average Email Delivery Time (as defined above)	**Service Credit**
> 2	25%
> 4	50%
> 10	100%

7. Message Filtering Virus SLA - 100% known virus detection and blocking
Definition: The detection and blocking of known viruses by the filters to prevent infection. “Viruses” is broadly defined as known malware, which includes viruses, worms, and Trojan horses. For classification of malware, please visit http://www.microsoft.com/technet/security/topics/serversecurity/avdind_2.mspx

7.1 A virus is considered known when a Message Filtering virus scanning engine can detect the virus and the detection capability is available throughout the Message Filtering network

7.2 Must result in a non-purposeful infection

7.3 The virus must have been scanned by the Message Filtering virus filter

7.4 If Message Filtering delivers an email that is infected with a known virus to Customer, Message Filtering will notify customer and work with customer to identify and remove the virus. If this results in the prevention of an infection, the remedy does not apply.

7.5 This SLA shall not apply to:

7.5.1 Forms of email abuse not classified as malware, such as spam, phishing and other scams, adware, and spyware. For classification of malware, please visit http://www.microsoft.com/technet/security/topics/serversecurity/avdind_2.mspx

7.5.2 Corrupt, defective, truncated, or inactive viruses contained in NDRs, notifications, or bounced emails.

7.6 Remedy:

7.6.1 25% service credit if an infection occurs in a calendar month, with a maximum of one claim allowed per calendar month.

8. Message Filtering Spam Effectiveness SLA – 95%
Definition: The percentage of inbound spam detected by the filtering system for Customer in a calendar month, measured in days.

8.1 Spam effectiveness estimates exclude false negatives to invalid mailboxes

8.2 The spam message must be processed by Sprint’s service and be non-corrupt, malformed, or truncated.

8.3 This SLA shall not apply to email containing a majority of foreign language content

8.4 Customer acknowledges that classification of spam is subjective and accepts that Sprint will make a good faith estimation of the spam capture rate based on evidence timely supplied by Customer.

8.5 Remedy – see table:

Spam Effectiveness SLA	
% of Calendar Month that Spam Capture rate is below 95%	**Service Credit**

> 25%	25%
> 50%	50%
100%	100%

9. Message Filtering False Positive SLA – 1:250,000
Definition: The ratio of legitimate business email incorrectly identified as spam by the filtering system to all email processed by the service for Customer in a calendar month.

9.1 Complete, original message, including all headers, must be reported to the abuse team within five (5) calendar days of message delivery

9.2 Applies to email sent to valid mailboxes only

9.3 Customer acknowledges that classification of false positives is subjective and understands that Sprint will make a good faith estimation of the false positive ratio based on evidence timely supplied by Customer.

9.4 This SLA shall not apply to:
9.4.1 bulk, personal, or pornographic email
9.4.2 email containing a majority of foreign language content
9.4.3 email blocked by a policy rule, reputation filtering, or SMTP connection filtering

9.5 Remedy – see table:

False Positive SLA	
False Positive Ratio in a Calendar Month	**Service Credit**
> 1:250,000	25%
> 1:10,000	50%
> 1:100	100%

10. DISCLAIMERS AND LIMITATIONS OF LIABILITY.

10.1 IN NO EVENT SHALL SPRINT OR ITS SUPPLIERS/LICENSORS BE LIABLE TO CUSTOMER WHETHER IN CONTRACT OR IN TORT FOR ANY LOST PROFITS, LOSSES RESULTING FROM MISSING, CONTAMINATED OR MISDIRECTED EMAIL MESSAGES OR MESSAGE CONTENTS, LOSSES OR EXPENSES RELATING TO INTERRUPTION OF BUSINESS ACTIVITIES, OR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER UNDER THIS ANNEX OR OTHERWISE, EVEN IF SPRINT WAS ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

11. TERMINATION. In addition to the termination rights set forth in the Standard Terms and Conditions for Communications Services or the Agreement, Sprint reserves the right at Sprint's option to terminate or suspend performance under this Agreement and discontinue providing Services to Customer in the event Customer materially or repeatedly fails to comply with Sprint's AUP. In such an event, Sprint shall attempt to notify Customer of any violation prior to termination or suspension of this agreement so that Customer may have opportunity to cure such failure. Sprint reserves the right to take immediate action to suspend any aspect of the Services provided to the Customer if Sprint determines that the violation or threatened violation of the AUP involves illegal or illicit activities or activities that are materially damaging to Sprint or substantially offensive to Sprint or its other customers.

12. MODIFICATION OF SERVICES. Sprint reserves the right to modify the features and functionality of the Services, at no additional cost to Customer, with the objective of providing Customer with equal or enhanced services.

13. SERVICES SUMMARY. The specific services included in each service packages are listed below. The services will be provided based on the service package subscribed to by the Customer as documented in the "Order". All Sprint Message Protection services include Web Reports and Web Administration.

13.1 Message Filtering
13.1.1 Inbound Content Blocking and Policy Management
13.1.2 Anti-Virus Management Service

13.1.3 Spam Management Service (including Message Quarantine Service)
13.1.4 Disaster Recovery (“Store & Forward”)
13.1.5 Outbound Anti-Virus Management & SMTP Services
13.1.6 Outbound Content Blocking and Policy Management

13.2 Message Archive
13.2.1Compliance
13.2.2 Organizations leverage a central archive repository for their specific requirements

13.3 Message Continuity
13.3.1 Disaster Recovery Management Tools
13.3.2 End users access mailboxes through security-enhanced Web browser

13.4 Message Encryption
13.4.2 TLS-enabled network
13.4.1 Policy-based encryption
13.4.2 IBE technology for public key
13.4 3 Web-based decryption and encrypted replies

14. SERVICE DESCRIPTIONS. The detailed descriptions of each service are listed below.

14.1 MESSAGE FILTERING

14.1.1 Virus Protection Features

Message Filtering help protect customers email platforms from all known viruses and helps provide zero-day threat protection against virus outbreaks. Multiple antivirus engines are integrated at the application programming interface level to continually provide critical virus definition updates. Message Filtering uses minimum of three different antivirus engines at all times with the ability to immediately engage additional engines when acute threats warrant additional coverage.

14.1.2 Spam Protection Features

Message Filtering virtually eliminates spam from inboxes using multiple filtering engines. Captured spam is routed to the spam quarantine and can be accessed by administrators or end users at any time through an intuitive Web-based interface. An e-mail notification listing quarantined spam can be configured to send to each valid e-mail address making it simple and effective to review spam. A spam quarantine Web-based interface and HTML notifications are available in several languages.

14.1.3 Policy Enforcement

Administrators have the ability to setup and enforce policies to comply with corporate policies on e-mail usage and with government regulations such as the Gramm-Leach-Bliley Act, SEC Rule 17a, NASD Rules 3010 and 3110, and the Health Insurance Portability and Accountability Act). An intuitive policy rule writer is available to monitor and manage e-mail messages based on message attributes, such as originating IP, sender, recipient, message size, file attachment, or specific text in the subject or body.

14.1.4 Disaster Recovery

The Disaster Recovery feature helps to ensure that no e-mail is lost or bounced if the Customer’s e-mail server or Internet connection becomes unavailable. Inbound e-mail is queued in a secure environment for up to five days and when the customer’s e-mail servers recover, all queued e-mail is automatically forwarded in a flow-controlled fashion. In cases of extended downtime, e-mail can be rerouted to another server or made available through a Web-based interface.

14.2 MESSAGE ARCHIVE

Message Archive service intercepts all inbound and outbound email in real time and uses proprietary technology to parse, tag, and index each message. Message Archive serializes each message to assure messages are captured according to regulatory specifications. All messages are stored in a database that is available online and searchable for the length of the customer’s storage agreement, typically three, five or seven years, as dictated by the customer’s archiving requirements. Message are processed and stored in a primary and secondary data center so redundancy of storage and processes exists, providing regulatory compliance, failover and disaster recovery. Internal email which is transmitted within a company’s email system (i.e., via Microsoft Exchange) are routed to Message Archive via the mail system’s archiving or journaling capability to store copies “in stream”. Historical data (SSL) is a one-time charge $66.00 per Gigabyte load of historical data.

14.2.1 Inbound Features include

14.2.1.1 Create archived copy and index
14.2.1.2 Send messages through to recipients

14.2.2 Outbound Features include:

14.2.2.1 Create an archived copy and index
14.2.2.2 Append disclaimer
14.2.2.3 Send through to recipient

14.2.3 Business Continuity & Disaster Recovery Features include:

14.2.3.1 Access email
14.2.3.2 Recover fully from disaster
14.2.3.3 Receive, reply and create email if system is down

14.2.4 Legal Discovery Features include:

14.2.4.1 Full message search including attachments
14.2.4.2 Tagging & extraction

14.2.5 Compliance Features include:

14.2.5.1 Random sampling of messages
14.2.5.2 Keyword phrase matching
14.2.5.3 Monitor, review, log, & report

14.3 MESSAGE CONTINUITY

Message Continuity allows the Customer’s end users to access their email by logging into a security-enhanced Web browser during planned or unplanned outages. End users have the ability to compose, receive, and send messages in real time with access to the entire company directory for addressing internal messages. The message repository is filtered upstream by the Message Filter module mentioned above. Thirty (30) days of previous e-mail is searchable and available to be restored to the primary mailbox and Disaster Recovery Manager Tools are built into the system to assist with communication, message management and user administration.

14.4 MESSAGE ENCRYPTION

Message Encryption is deployed over the Internet enabling the Customer’s end users to send and receive encrypted e-mail.

14.4.1 Transparent Encryption and E-Mail Delivery

When an e-mail is sent it travels through the Internet through a TLS-encrypted tunnel, and is automatically encrypted at the gateway according to policy rules created and managed within the Message Filtering module. When a message is encrypted, a private key for the recipient is created and stored in a secure environment on the Internet. The private key is made available to the message recipient when the recipient decrypts the message. The recipient does not have to pre-enroll to receive and decrypt the message. The encryption process is transparent to the sender, who does not need to do anything other than write and send the message as usual.

14.4.2 Simple Authentication and Security-Enhanced, Web-based Decryption

Upon receipt of a Message Encryption message, the recipient authenticates their identity and sets a password to securely open encrypted messages from the Message Encryption service. Once this password is created, the recipient can use the same password to authenticate and view protected email.