PAETEC

WEB SECURITY TERMS AND CONDITIONS

In addition to the general terms and conditions contained in the Service Agreement between PAETEC and Customer (the "Agreement"), of which these Web Security Terms and Conditions are a part, Customer agrees that the following terms and conditions apply to the Web Security Service provided to Customer by PAETEC.

A. **Web Security Service and Charges**. During the Term this Schedule is in effect, as set forth herein, PAETEC will provide Internet-level Web Security Service as selected by the Customer and as described in this Schedule and the attached Appendices (the "Web Security Service") to the Customer in accordance with the terms and conditions of this Schedule, at the prices shown on the Rate Schedule to the Agreement. For the Web Security Service, any IP change or addition shall be $75.00 per change or addition.

B. **Configuration Requirements:** PAETEC must receive the following information from Customer prior to the provisioning the Web Security Service.

1. **Customer's IP Range**. In order for PAETEC to filter Customer's web traffic, the Web Security Service must be configured with Customer organization's externally facing IP address(es) (The external static IP address(es) provided by Customer's ISP). If there are multiple sites with separate internet gateways for web browsing, all site IP addresses must be provided to PAETEC.

2. **Proxies, Caches, and Firewalls**. If Customer is using an internal web proxy (e.g. Microsoft ISA server, squid, etc) Customer must provide the Product & Version information to PAETEC.

3. **User-Level Granularity, Reporting and Control**. User granularity and control of reporting requires Customer to be using Windows 2000 or later, and an LDAP-enabled Active Directory-based network. Customer is also required to install a Client Site Proxy and a LDAP Web User Synchronization Tool. Customers will be notified when the Proxy and Synchronization Tools are available. Only Customers who subscribe to the per user pricing option (not the bandwidth pricing option) of the Web Security Service will be eligible to receive user level granularity reporting.

C. **Additional Configuration Requirements relative to Web/Email Protector security bundle:**

1. **Customer's Inbound Email Configuration**. If Customer elects to receive the Web/Email Protector security bundle, in order for PAETEC to scan Customer's inbound e-mail, the Web Security Service must be configured to know which domains to scan. After an e-mail has successfully passed through the network control towers, it is transferred to Customer's nominated SMTP mail server(s) using the domain name and associated mail host name. The IP Address should be the externally visible IP Address.

2. **Customer's Outbound E-Mail**. If Customer elects to receive the Web/Email Protector security bundle, in order for PAETEC to scan Customer's outbound e-mail, the Web Security Service must be configured to accept e-mail from the Firewall, Router or Mail Server Customer uses for outbound e-mail. PAETEC requires a list of all IP Addresses that Customer currently sends its outbound email from to properly provision the Web Security Service.

D. **SPAM Manager Service – Email Portion Configuration**. If Customer elects to receive the Web/Email Protector security bundle, Customer may elect to receive the Spam Manager Service under the following terms:

1. If Customer elects Spam Manager Service for a domain, Customer's account will be set up automatically upon the first time that suspected Spam is identified by the Spam Manager Service. Customer will automatically receive an e-mail notification with instructions on how to access and use the interface through which Spam Manager Service is administered.

2. Customer's Spam Manager Service account is accessible only by Customer.

3. Suspected Spam can be stored for a maximum of fourteen (14) days after which it will be automatically deleted.

4. If for any reason the Spam Manager Service is not able to accept e-mail, the suspected Spam will be tagged and sent to the recipient as per the following: Options are available for Customer to determine the actions to be taken by PAETEC upon the detection of possible Spam e-mail. These options, in order of increasing severity, are: (x) Tag such e-mail within it's header; (y) Redirection of such e-mail to a pre-determined e-mail address; or (z) Deletion of such e-mail.

E. **Web/Email Protector Provision of Service**. If Customer elects to receive the Web/Email Protector security bundle, Customer will be contacted by PAETEC shortly after Customer's order has been processed with the account information needed for the administrator to set up the Web Security Service so that Customer's e-mail can be scanned. Customer is responsible for ensuring that its company makes such changes.

1. **Customer's Inbound E-mail**
   To have Customer inbound e-mail virus scanned, it is necessary for the MX records of the relevant domain names to be changed to direct Customer's inbound e-mail to the network Control Towers. Instructions on how to achieve this will be sent by e-mail to Customer once Customer's order has been processed.

2. **Customer's Outbound E-mail**
   Once the Web Security Service is configured to scan Customer's outbound e-mail, Customer must configure its mail servers to relay all outbound e-mail to the network Control Towers. The host name of the appropriate Control Towers will be sent to Customer by e-mail once Customer's order has been processed.

F. **Customer Shared E-mail Hosting**. PAETEC will not be scanning e-mail that is received from a Customer shared e-mail hosting environment.

G. **General Terms and Conditions Applicable to the Web Security Service**:
In addition to the specific General Terms and Conditions set forth on the applicable schedule(s) herein, the follow terms and conditions apply to the Web Security Service.

1. **No Resale.** Customer is prohibited from reselling, subleasing or sublicensing the Service. The intellectual property rights in the Service and any hardware of software used in connection with the Service is and will at times remain the property of PAETEC or its licensor of the Service.

2. **Termination.** If Customer terminates the Service, except for terminations for cause as permitted under the Agreement, Customer shall be liable to PAETEC for an early termination charge equal to the contracted number of users times the monthly user fee times the remaining months in the Term. Should the Service be suspended or terminated for any reason whatsoever, PAETEC shall reverse all configuration changes made upon provisioning of the Service and it shall be the responsibility of the Customer to undertake all necessary configuration changes to its mail servers and domain name and to inform their ISP of the need to reroute inbound e-mail.

3. **Limitation of Liability.** NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, THE SERVICE IS PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTIES WHATSOEVER AND PAETEC AND/OR ITS VENDOR OF THE SERVICE DISCLAIM ALL WARRANTIES EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMER'S TERMINATION RIGHTS AS SET FORTH HEREIN AND IN THE AGREEMENT ARE CUSTOMER'S SOLE REMEDY AND PAETEC'S SOLE LIABILITY IN THE EVENT OF ANY PROBLEM WITH THE SERVICE.

4. **Compliance with AUP.** Customer agrees to adhere at all times to the PAETEC Acceptable Use Policy (the "AUP"); as such AUP may be modified by PAETEC from time to time. The current AUP is available for review at http://www.PAETEC.com/aup. PAETEC has the right to modify its AUP at any time without prior notice to Customer. Customer is responsible for monitoring the website at http://www.PAETEC.com/aup for changes to the AUP. Customer shall be bound by such modified AUP. PAETEC has the right to immediately and without regard to any cure periods that may be set forth elsewhere in the Agreement, suspend and/or terminate the Services to Customer, or to take any other action that PAETEC determines, in its sole discretion, is appropriate in response to Customer's failure to comply with the requirements of PAETEC's then-current AUP.

5. **Other**. Upon expiration of the Term, Service shall continue to be provided on a month-to-month basis, cancelable on thirty days' prior written notice. Charges for the Service shall relate to the number of Users and domains being scanned by the Service ("Registered Usage"). Customer must notify PAETEC if at any time the number of Users being scanned by the Service exceeds the then Registered Usage or if additional domains are being added to the Service. PAETEC will monitor Customer's actual usage and if the number of Users or domains being scanned exceeds the then Registered Usage, PAETEC will have the right to charge for additional usage fees during the Customer's next bill cycle after quarterly true up. No reduction in the numbers of Users or domains being scanned is permitted during the initial Term.

Customer must notify PAETEC in writing at least thirty days' prior to any change in Customer's Internet Service Provider and provide updated contact information in order for the Service to work properly.

Appendix 1
Web Anti Spyware and Anti Virus

Overview

(a) Once the relevant configuration requirements are met as hereinabove set forth, and setup has been completed, requests for Web pages and attachments are electronically routed via the Web Anti Spyware and Anti Virus ("WebASAV") and digitally examined for viruses.

Service Description

(a) The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Web Security Service. Other content routed though HTTP (for example streaming media) can also be passed through the Web Security Service but shall not be scanned.
(b) WebASAV will scan the complete file item.

Configuration

(a) The configuration settings required to direct this external traffic via the Web Security Service are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via the Web Security Service. Where the Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of the Customer to make the necessary changes to their own infrastructure to facilitate this.
(b) Access to the Web Security Service is restricted via Scanning IP i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the Customer and dynamically select Customer-specific settings.
(c) WebASAV will scan as much of the Web page and its attachments as possible. It may not be possible to scan certain Web pages, content or attachments (for example, password protected). Attachments specifically identified as unscannable will not be blocked. Streamed and encrypted traffic (i.e. Streaming Media and/or HTTPS/SSL) cannot be scanned and will be passed through Web ASAV unscanned.

Alerts

(a) If a Customer's Web page or attachments are found to contain an item identified as a Virus, Spyware or Adware, then access to that Web page or attachment is denied and the Internet user will be displayed an automatic alert Web page and/or optional email alert in accordance with the specification below. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page and the alert page may replace the content of the requested item, but access to the infected page or attachment will still be denied.

General Terms and Conditions

(a) NO WEB SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE PAETEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF WebASAV TO DETECT VIRUSES, MALICIOUS CODE, SPYWARE OR ADWARE.
(b) PAETEC emphasizes that the configuration of WebASAV is entirely in the control of the Customer. The services described in this Appendix are intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel and so PAETEC advises the Customer to always check their local legislation prior to deploying WebASAV. PAETEC can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of WebASAV.

Appendix 2
Web URL Filtering

Overview

(a) Once the relevant configuration requirements are met as hereinabove set forth, and setup has been completed, requests for Web pages and attachments are electronically routed via Web URL Filtering ("WebURL") and digitally examined.

Service Description

(a) The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Web Security Service.

Configuration

(a) The configuration settings required to direct this external traffic via the Web Security Service are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via the Web Security Service. Where the Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of the Customer to make the necessary changes to their own infrastructure to facilitate this.

(b) Access to the Web Security Service is restricted via Scanning IP i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the Customer and dynamically select customer-specific settings.

(c) The Customer is able to configure WebURL to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Users or groups.

Alerts

(a) If a User requests a Web page or attachment where an access restriction policy applies, then access to that Web page or attachment is denied and the User will be displayed an automatic alert Web page and/or optional email alert in accordance with the specification below. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page and the alert page may replace the content of the requested item, but access to the relevant page will still be denied.

Reporting

(a) To enable per User or group administration and reporting, the Customer is required to install the relevant software application (the "Client Proxy") in accordance with the installation guidelines. Use of the Client Proxy is subject to the End User License Agreement provided with the Client Proxy.

General Terms and Conditions

(a) NO WEB SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE PAETEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF WebURL TO DETECT BLOCKED URLs OR CONTENT.

(b) PAETEC emphasizes that the configuration of WebURL is entirely in the control of the Customer. The services described in this Appendix are intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel and so PAETEC advises the Customer to always check their local legislation prior to deploying WebURL. PAETEC can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of WebURL.

Appendix 3
Web/Email Protector Security Bundle

Overview

(a) Once all relevant configuration requirements are met as hereinabove set forth, and setup has been completed, all requests for Web pages and Inbound / Outbound Email are electronically routed via the scanning servers and are digitally examined before forwarding.

Service Description

(a) PAETEC's Web/Email Protector is a bundled service that includes the following:

- Email Scanning Anti Virus
- Email Scanning Anti Spam
- Web Security Anti Spyware scanning
- Web Security Anti Virus scanning
- 1.5Mb Internet port.

Configuration

(a) Configuration requirements include those set out within these Web Security Terms and Conditions, including Appendix 1 (Web Anti Spyware and Anti Virus) as well as relevant Internet port configuration requirements.

Alerts

(a) If a Customer's Web page or attachments are found to contain an item identified as a Virus, Spyware or Adware, then access to that Web page or attachment is denied and the Internet user will be displayed an automatic alert Web page and/or optional email alert in accordance with the specification below. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page and the alert page may replace the content of the requested item, but access to the infected page or attachment will still be denied.

General Terms and Conditions

(a) NO SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE PAETEC CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE WEB/EMAIL PROTECTOR SERVICE.

(b) **No Open Relay.** Customer's order will not be processed if Customer's mail server allows open relay. PAETEC will test Customer's mail server before Customer receives the Service, and on a regular basis thereafter, to ensure Customer's mail server does not support open relay. Should PAETEC find that Customer's mail server allows open relay or is blacklisted or if Customer's name appears on any list of known spammers, PAETEC reserves the right to suspend the Service immediately. PAETEC will work with Customer to get the problem rectified as soon as possible and reinstate the Service once the problem has been rectified.

Appendix 4
Web Security Service SLA

Web Security Service Availability

1. This Web Security Service Availability SLA will only operate if the Customer utilizes one or more of the Web Security Services, and shall not apply to the Web/Email Protector Security Bundle portion of the Web Security Service.

2. "Web Security Service Availability" means the availability of the Customer's designated Web Security Services tower or secondary tower(s) to accept the Customer's outbound web requests from a correctly configured Customer host on behalf of the Customer on a 24x7 basis, subject to correct configuration by the Customer of their hosts or gateway devices or proxy(s) as per PAETEC's guidelines (available upon request). Measurement of Web Security Service Availability will be via the PAETEC tracker.

3. If in any calendar month Web Security Service Availability is below one hundred percent (100%) the Customer may be entitled to a percentage credit in accordance with the table below.

Percentage Web Security Service Availability per calendar month as Determined by PAETEC	**Percentage credit of the Web Security Service Monthly Recurring Charge**
< 100% but > 99.0%	**20**
< 99.0% but > 98.0%	**40**
< 98.0% but > 97.0%	**60**
< 97.0% but > 96.0%	**80**
< 96.0% but > 95.0%	**100**
< 95.0%	**Termination of the Web Security Service by Customer upon 30 days prior written notice to PAETEC.**

4. **Maximum Credit.** In no event may the credits provided for hereunder (either individually or on a cumulative basis) in any billing period exceed the total monthly recurring charges for the Web Security Service for that period.