

Service Description

IBM Managed Security Services for Web Security

1. Scope of Services

IBM Managed Security Services for Web Security (called "MSS for Web Security" or "Service") may include:

- a. Web Antivirus and Web Antispyware services to help Customer detect Viruses and Spyware in response to the Requests for Web pages and attachments issued by Customer's users; and/or
- b. Web URL Filtering service to help prevent access to certain Web pages or attachments, by Customer's users (in line with Customer's access restriction policy).

MSS for Web Security is intended to help Customer enforce an appropriate computer use policy.

The details of Customer's order (for example, the services required, contract period and charges) will be specified in an Order.

Definitions of Service-specific terminology can be found at www.ibm.com/services/iss/wwcontracts.

2. Definitions

Designated Tower Cluster – a cluster of towers (minimum of two), designated to provide MSS for Web Security to Customer.

Known Virus – a Virus for which at the time of receipt of the content by IBM: (i) a signature has already been made publicly available for a minimum of one hour for configuration by third party commercial scanners used by IBM; or (ii) is included in the "Wild List" held at <http://www.wildlist.org> and identified as being "In the wild" by a minimum of two Wild List participants.

Planned Maintenance – maintenance periods which cause disruption of the services due to non-availability of the Designated Tower Cluster. Notice will be provided to Customer a minimum of five calendar days prior to such maintenance. Planned Maintenance shall not exceed more than eight hours per calendar month and will not take place during the Customer's local business hours.

Request – a request by a user for Web content (such as a Web page) via a Web browser or similar HTTP tool, from any Web server connected to the Internet.

Spyware – software or tools that covertly gather information, typically about user or system activity, without the knowledge or consent of the user or organization.

Virus – program code that plants itself in a file or memory, infects other files and memory areas, and runs without authorization.

Web Latency – the measured time from when IBM receives the content to the point of attempted transmission of the content.

Web Service Availability – the availability of the Web Services to accept the Customer's outbound web requests.

3. MSS for Web Security

3.1 MSS for Web Security Coordination

3.1.1 IBM Responsibilities

IBM will provide a deployment engineer who will be the IBM focal point during the initialization and notification phase of MSS for Web Security. The deployment engineer will:

- a. provide you with a customer profile, which Customer must complete prior to IBM providing MSS for Web Security;
- b. review this Service Description, and any associated documents, with Customer Point of Contact;
- c. coordinate and manage the technical activities of the IBM assigned personnel; and
- d. establish and maintain communications through Customer Point of Contact during the initialization and notification phase of MSS for Web Security.

3.1.2 Customer Point of Contact Responsibilities

Prior to the start of MSS for Web Security, Customer will designate a person (called "Customer Point of Contact"), to whom all communications relative to MSS for Web Security will be addressed and who will have the authority to act on Customer's behalf in all matters regarding the Service. Customer Point of Contact will:

- a. complete and return the customer profile to IBM within ten business days of receipt;
- b. serve as the interface between the IBM Service team and all of Customer's departments participating in MSS for Web Security, as well as any third-party vendors, including Internet Service Providers ("ISPs") and content-hosting firms, used by Customer to implement its Internet presence;
- c. obtain and provide applicable information, data, consents, decisions and approvals as required by IBM to perform the Service, within two working days of an IBM request; and
- d. help resolve Service issues, and escalate issues within Customer's organization, as necessary.

3.1.3 Customer General Responsibilities

The IBM performance of MSS for Web Security is dependent on Customer's performance of these general responsibilities. Customer agrees to:

- a. provide all necessary equipment and software and pay communication charges to access the IBM Web portal or any other Web tool required for provision of the Service;
- b. make appropriate personnel available to assist IBM in the performance of the IBM responsibilities;
- c. permit IBM to disclose this document and the associated Order to its subcontractors, in connection with the Service to be performed hereunder;
- d. be responsible for the content of any database, the selection and implementation of controls on its access and use, backup and recovery and the security of the stored data. This security will also include any procedures necessary to safeguard the integrity and security of software and data used in the Service from access by unauthorized personnel; and
- e. be responsible for the identification and interpretation of any applicable laws, regulations, and statutes that affect Customer's existing software and data to which IBM will have access during delivery of the Service. It is Customer's responsibility to ensure that the software and data meet the requirements of those laws, regulations and statutes.

3.2 General Services

3.2.1 IBM Responsibilities

IBM will:

- a. provide Customer with password access to a proprietary Internet-based reporting and management tool to allow Customer to view data and statistics on its use of the Service. This tool will also offer a number of configuration and management facilities;
- b. provide the Service on a 24 hours/day by 7 days/week basis;
- c. provide access to software, such as a client-side proxy and a Lightweight Directory Access Protocol ("LDAP") synchronization tool, that may be required for some optional Service features;
- d. provide technical support for the Service on a 24 hours/day by 7 days/week basis; and
- e. work remotely with Customer on a 24 hours/day by 7 days/week basis to resolve problems with the Service.

3.2.2 Customer Responsibilities

Customer agrees to:

- a. monitor the number of users and notify IBM if the actual number of users exceeds the number ordered. IBM and Customer will work to upgrade the Order to include the additional users;
- b. manage and maintain any optional software provided by IBM in support of the Service;
- c. provide all technical data and other information IBM may reasonably request from time to time to allow IBM to supply the Service to Customer;
- d. maintain the security of the password provided to Customer for access to the proprietary Internet-based configuration, management and reporting tool, including not disclosing to any third party; and

- e. provide IBM with the name, telephone number and e-mail address of Customer's Web administrator, if Customer has selected this option in the customer profile.

3.2.3 General Service Level Agreements

The general service level agreement ("SLA") guarantees described below comprise the measured metrics for delivery of the Service. Unless explicitly stated below, no additional guarantees or warranties of any kind shall apply to services delivered under this Service Description. The sole remedies for failure to meet the general SLA guarantees are specified in the section entitled "General SLA Remedies" below.

Service levels are not applicable:

- a. until 30 days after activation of the Service;
- b. if Customer system configurations do not comply with the provided configuration guidelines;
- c. during periods of Planned Maintenance; or
- d. during periods of non-availability due to force majeure.

General SLA Guarantees

- Web Service Availability guarantee - IBM will maintain Service availability for 100% of the calendar month.

The Web Service Availability guarantee is only applicable if the Customer host, gateway devices or proxy(s) are correctly configured on a 24x7 basis.

- Web Latency guarantee – IBM will deliver content with an average latency of 100 milliseconds or less.

The Web Latency guarantee is only applicable to objects of 1 MB or less.

All credit requests must be submitted to IBM within five days after the end of the month in which the eligibility occurred. Credit eligibility is subject to verification by IBM.

General SLA Remedies

The general SLA remedies are available provided Customer meets its obligations as defined in this Service Description.

A credit will be issued as the sole remedy for failure to meet either of the guarantees described in the section entitled "SLA Guarantees", during any given calendar month. Customer may obtain no more than 100% of the monthly charge, in a given calendar month. Payment of Service credits shall be considered liquidated damages and are the Customer's sole and exclusive remedy.

- Web Service Availability remedy - If the Web Service Availability is below 100% in any calendar month during the contract period, a credit will be issued as follows:

Percent Web Service Availability per Calendar Month	Percent Credit of Monthly Charge
Less than 100% but greater than 99.0%	25
Less than 99.0% but greater than 98.0%	50
Less than 98%	100 Termination of Service at Customer's discretion. Should the Service be terminated, such termination shall be the sole and exclusive remedy with respect to availability of the Service for less than 98% in a given calendar month.

- Web Latency remedy - If the average scanning time of Web content calculated over the course of any calendar month is less than 100%, credit will be issued in accordance with the following table:

Average Percentage of Web Content Scanning within 100 Milliseconds	Percent Credit of Monthly Charge
Less than 100% but greater than 99.0%	25
Less than 99.0% but greater than 98.0%	50
Less than 98.0% but greater than 97.0%	75
Less than 97%	100 Termination of the Service at Customer's discretion. Should the Service be terminated, such termination shall be the sole and exclusive remedy with respect to Web Latency.

3.3 Web Antivirus and Web Antispyware

If selected by Customer in an applicable Order, IBM will provide Web Antivirus and Web Antispyware to assist Customer in detecting Viruses and Spyware in both inbound and outbound Hyper Text Transfer Protocol (“HTTP”) and File Transfer Protocol (“FTP”)–over-HTTP Requests for Web pages and attachments. Web Antivirus and Web Antispyware services are limited to the number of users specified in the Order.

3.3.1 IBM Responsibilities

Activity 1 - Initialization and Notification

IBM will provide access to Web Antivirus and Web Antispyware via the IP Addresses from which Customer’s Web traffic originates (“scanning IPs”). Customer’s scanning IPs will be used to identify its Web traffic and to select its specific settings. IBM will not perform scans on files or content that does not originate from Customer’s scanning IPs.

Activity 2 - Technical and Ongoing Support

During the contract period, IBM will:

- a. direct external HTTP and FTP-over-HTTP files and content originating from Requests (including all attachments, macros or executables) through MSS for Web Security. Other content routed through HTTP (i.e., streaming media and/or HTTPS/SSL) may also be passed through MSS for Web Security, but will not be scanned for Viruses or Spyware;
- b. scan each file or content transfer resulting from each Request. If no infections are found, the file or content will be passed through;
- c. deny user access to a file (for example, a Web page or attachment) in which a Virus or Spyware is detected or that is considered to be unscannable (with the exception of secure socket layer traffic). In such event, IBM will attempt to display an automatic alert regarding the infected Web page to the user; and
- d. notify the user and, if requested by Customer, a Web administrator, of a file download found to contain a Virus or Spyware in Customer’s Internet communications.

3.3.2 Customer Responsibilities

Customer agrees to:

- a. implement and maintain the configuration settings required to direct external traffic through MSS for Web Security; and
- b. ensure its internal HTTP and FTP-over-HTTP traffic is not directed via Web Antivirus and Web Antispyware. If Customer’s Internet service mandates a direct connection rather than via a proxy, it is Customer’s responsibility to make the necessary changes to its infrastructure to facilitate such direct connection.

3.3.3 Service Level Agreements

The SLA guarantee described below comprises the measured metrics for delivery of Web Antivirus. Unless explicitly stated below, no additional guarantees or warranties of any kind shall apply to services delivered under this Service Description. The sole remedies for failure to meet the SLA guarantees are specified in the section entitled “SLA Remedies”, below.

The SLA remedies are available provided Customer meets its obligations as defined in this Service Description.

SLA Guarantees

- Known Virus Protection guarantee – IBM will block all Known Viruses. This SLA applies only to version 2 of the Web Antivirus service.

Customer’s systems will be deemed to be infected if a Known Virus, contained in a Web transaction received through version 2 of the Web Antivirus service, has been activated within Customer’s systems, either automatically or with manual intervention.

If a Web transaction containing a Known Virus is detected but not stopped, to avoid application of the SLA, IBM may promptly notify Customer and provide sufficient information to enable Customer to identify and delete the item. If infection is prevented, this SLA will not apply. If Customer fails to promptly act on notice of an item infected with a Known Virus, this SLA will not apply.

IBM will scan as much of the downloaded Web item as possible. It may not be possible to scan items that are encapsulated or tunneled for communication purposes via the supported Web Protocols (HTTP, and FTP-over-HTTP), conveyed over HTTPS, compressed or modified from their original form for distribution, product license protection, download or update, or content which is under the direct control of the sender (for example, password protected and/or encrypted items). Such items and/or attachments are excluded from this SLA.

SLA Remedies

- Known Virus Protection remedy – If Customer's systems are infected by one or more Viruses in a single calendar month during the contract period, IBM will issue a credit for the lesser of: (i) 100% of the monthly charge for the Web Antivirus service or (ii) \$10,000 U.S. (or equivalent in local currency). Such credit will only apply if Customer has provided notice to IBM, and IBM has confirmed and logged that a Virus has been passed to Customer through the Service. This remedy shall not apply to any deliberate self-infection by Customer.

3.4 Web URL Filtering

If selected by Customer in an applicable Order, IBM will provide Web URL Filtering to assist Customer in denying user access to a Web page or attachment inline with Customer's access restriction policy. Web URL Filtering is limited to the number of users specified in the Order.

3.4.1 IBM Responsibilities

Activity 1 - Initialization and Notification

IBM will provide access to Web URL Filtering via the IP Addresses from which Customer's Web traffic originates ("scanning IPs"). Customer's scanning IPs will be used to identify its Web traffic and to select its specific settings. IBM will not perform scans on files or content that does not originate from Customer's scanning IPs.

Activity 2 - Technical and Ongoing Support

During the contract period, IBM will:

- a. direct external HTTP and FTP-over-HTTP files and content resulting from Requests (including all attachments, macros or executables) through Web URL Filtering; and
- b. deny access to a URL, Web page or attachment where an access restriction policy applies. In such event, IBM will attempt to display an automatic alert regarding the inappropriate URL or Web page to the user.

3.4.2 Customer's Responsibilities

Customer agrees to:

- a. configure Web URL Filtering to include its access restriction policies, which should be based both on categories and types of content;
- b. distribute and create its access restriction policies (based both on categories and types of content);
- c. implement and maintain the configuration settings required to direct external traffic via Web URL Filtering; and
- d. ensure that internal HTTP and FTP-over-HTTP traffic is not directed via Web URL Filtering. If Customer's Internet service mandates a direct connection rather than via a proxy, it is Customer's responsibility to make the necessary changes to its infrastructure to facilitate such direct connection.

4. Disclaimer/Warranty

Customer understands and agrees that IBM does not make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information provided as part of the Service.

5. Other Terms and Conditions

IBM reserves the right to modify the terms of this Service Description at any time. Should such modification reduce the scope or level of the Service being delivered (for example, eliminating a previously provided Service or lengthening the Security Incident response time), IBM will provide a minimum of 30 days prior notice via the IBM Web portal or other electronic means.