IBM United Kingdom Limited
Registered in England: 741598
Registered Office: PO Box 41,
North Harbour, Portsmouth,
PO6 3AU (hereinafter "IBM")

Services Description

IBM Managed Security Services (Cloud Computing) - hosted e-mail and Web security - express managed Web security

IN ADDITION TO THE TERMS AND CONDITIONS SPECIFIED BELOW, THIS SERVICES DESCRIPTION INCLUDES THE "IBM MANAGED SECURITY SERVICES GENERAL PROVISIONS" ("GENERAL PROVISIONS") LOCATED AT http://www-935.ibm.com/services/uk/gts/html/contracts_landing.html AND INCORPORATED HEREIN BY REFERENCE.

1. Scope of Services

IBM Managed Security Services (Cloud Computing) - hosted e-mail and Web security - express managed Web security (called "Web Security" or "Services") is designed to help the Services Recipient enforce an appropriate computer use policy and may include:

a. Web Antivirus and Web Antispyware services to help the Services Recipient detect Viruses and Spyware in response to the Requests for Web pages and attachments issued by the Services Recipients; and/or

b. Web URL Filtering services to help prevent access to certain Web pages or attachments, by the Services Recipients (in line with the Services Recipient's access restriction policy).

The Services features described herein are dependent upon the availability and supportability of products and product features being utilised. Even in the case of supported products, not all product features may be supported. Information on supported features is available from IBM upon request. This includes both IBM-provided and non-IBM-provided hardware, software, and firmware.

2. Definitions

Alert Condition ("AlertCon") – a global risk metric developed by IBM, using proprietary methods. The AlertCon is based on a variety of factors, including quantity and severity of known vulnerabilities, exploits for such vulnerabilities, the availability of such exploits to the public, mass-propagating worm activity, and global threat activity. The four levels of AlertCon are described in the IBM Managed Security Services portal (called "Portal").

Education Materials – include, but are not limited to, lab manuals, instructor notes, literature, methodologies, electronic course and case study images, policies and procedures, and all other training-related property created by IBM. Where applicable, Education Materials may include participant manuals, exercise documents, lab documents and presentation slides provided by IBM.

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. Notice will be provided to the Services Recipient 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 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 organisation.

User – a person or machine that uses the Services

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

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

Web Services Availability – the availability of the Services to accept the Services Recipient's outbound Web requests.

3. Services

3.1 General Services

THE SERVICES DESCRIBED HEREIN ARE PROVIDED "AS IS" AND WITHOUT WARRANTY OR INDEMNITY OF ANY KIND BY IBM, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS.

3.1.1 IBM General Services Responsibilities

IBM will:

a. provide you with instructions on how to access software, such as a client-side proxy and a Lightweight Directory Access Protocol ("LDAP") synchronisation tool, that may be required for some optional Services features. Such software, which may include open source software and freeware, will be provided directly from a third party vendor and your use of this software will be subject to such vendor's end user license agreement ("EULA"), available for your review and acceptance prior to downloading the software. IBM is not a party to the EULA and IBM makes no representations and disclaims all express and implied warranties with respect to the software, and does not indemnify you against any claim that the software infringes a third party's intellectual property rights. UNDER NO CIRCUMSTANCES SHALL IBM BE LIABLE FOR ANY DAMAGES ARISING OUT OF YOUR USE OF SOFTWARE;

b. provide you with password access to a proprietary Internet-based reporting and management tool to allow you to view data and statistics on your use of the Services. This tool will also offer a number of configuration and management facilities;

c. provide the Services on a 24 hours/day by 7 days/week basis;

d. provide technical support for the Services on a 24 hours/day by 7 days/week basis.

3.1.2 Your General Services Responsibilities

You agree to:

a. monitor the number of Users, and notify IBM if the actual number of Users exceeds the number ordered or falls below the required minimum of ten Users. IBM will work with you to upgrade the Schedule to include the additional Users;

b. manage and maintain any optional software provided by IBM in support of the Services;

c. provide all technical data and other information IBM may reasonably request from time to time to allow IBM to supply the Services to you;

d. be bound by the terms and conditions set forth in the EULA which will be provided for your review and acceptance prior to your downloading of the software;

e. maintain the security of the password provided to you for access to the proprietary Internet-based configuration, management and reporting tool, including not disclosing to any third party;

f. provide IBM with the name, telephone number and e-mail address of your e-mail administrator, if you have selected this option in your profile; and

g. ensure the appropriate release authorisation form, to redirect e-mail to an alternate e-mail address is submitted to IBM in a timely manner.

3.2 Portal

The Portal provides you with access to an environment (and associated tools) designed to monitor and manage your security posture by merging technology and service data from multiple vendors and geographies into a common, Web-based interface.

The Portal may also be used to deliver Education Materials. All such Education Materials are licensed not sold and remain the exclusive property of IBM. IBM grants you a license in accordance with the terms provided in the Portal. EDUCATION MATERIALS ARE PROVIDED "AS IS" AND WITHOUT WARRANTY OR INDEMNITY OF ANY KIND BY IBM, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS.

3.2.1 IBM Portal Responsibilities

IBM will:

a. provide access to the Portal 24 hours/day, 7 days/week. The Portal will provide:

   (1) security intelligence awareness and alerting;

(2) a template-driven reporting dashboard; and

(3) access to Education Materials in accordance with the terms provided in the Portal.

3.2.2 Your Portal Responsibilities

You agree to:

a. utilise the Portal to perform daily operational Services activities;

b. ensure your employees accessing the Portal on your behalf comply with the Terms of Use provided therein including, but not limited to, the terms associated with Educational Materials;

c. appropriately safeguard your login credentials to the Portal (including not disclosing such credentials to any unauthorised individuals);

d. promptly notify IBM if a compromise of your login credentials is suspected; and

e. indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from your failure to safeguard your login credentials.

3.3 Security Intelligence

Security intelligence is provided by the IBM X-Force® Threat Analysis Center. The X-Force Threat Analysis Center publishes an Internet AlertCon threat level. The AlertCon describes progressive alert postures of current Internet security threat conditions. In the event Internet security threat conditions are elevated to AlertCon 3, indicating focused attacks that require immediate defensive action, IBM will provide you with real-time access into IBM's global situation briefing. As a user of the Portal, you have access to the X-Force Hosted Threat Analysis Service. The X-Force Hosted Threat Analysis Service includes access to the IBM X-Force Threat Insight Quarterly ("Threat IQ").

Utilizing the Portal, you can create a vulnerability watch list with customised threat information. In addition, each Portal user can request to receive an Internet assessment e-mail each business day. This assessment provides an analysis of the current known Internet threat conditions, real-time Internet port metrics data, and individualised alerts, advisories and security news.

NOTE: Your access and use of the security intelligence provided via the Portal (including the Threat IQ and the daily Internet assessment e-mail) is subject to the Terms of Use provided therein. Where such Terms of Use conflict with the terms of this Agreement, the Portal Terms of Use shall prevail over this Agreement. In addition to the Terms of Use provided in the Portal, your use of any information on any links or non-IBM Web sites and resources are subject to the terms of use posted on such links, non-IBM Web sites, and resources.

3.3.1 IBM Security Intelligence Responsibilities

IBM will:

a. provide you with access to the X-Force Hosted Threat Analysis Service;

b. provide you with a username, password, URL and appropriate permissions to access the Portal;

c. display security information on the Portal as it becomes available;

d. if configured by you, provide security intelligence specific to your defined vulnerability watch list, via the Portal;

e. if configured by you, provide an Internet security assessment e-mail each business day;

f. publish an Internet AlertCon via the Portal;

g. declare an Internet emergency if the daily AlertCon level reaches AlertCon 3. In such event, IBM will provide you with real time access into IBM's global situation briefing;

h. provide Portal feature functionality for you to create and maintain a vulnerability watch list;

i. provide additional information about an alert, advisory, or other significant security issue as IBM deems necessary; and

j. provide access to the Threat IQ via the Portal.

3.3.2 Your Security Intelligence Responsibilities

You agree to use the Portal to:

a. subscribe to the daily Internet security assessment e-mail, if desired;

b. create a vulnerability watch list, if desired,

c. access the Threat IQ, and:

d. agree to adhere to the licensing agreement and not forward Services information to individuals who do not have a proper license.

3.4 General Service Level Agreements

IBM Service Level Agreements ("SLAs") establish response time objectives and countermeasures for specific events resulting from the Services. The SLAs become effective when the deployment process has been completed, and support and management have been successfully transitioned to you. The SLA remedies are available provided you meet your obligations as defined in this Services Description and all associated contract documents.

SLAs are not applicable:

a. until 30 days after activation of Web Security;

b. if your 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 or acts or omissions by you, IBM, or a third party.

3.4.1 General SLA Availability

The SLA defaults described below comprise the measured metrics for delivery of the Services. Unless explicitly stated below, no warranties of any kind shall apply to Services delivered under this Services Description. The sole remedies for failure to meet the SLA defaults are specified in the section of this Services Description entitled "General SLA Remedies".

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

  The Web Services Availability SLA is only applicable if your host, gateway devices or proxy(s) are correctly configured on a 24 hours/day x 7 days/week basis.

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

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

3.4.2 General SLA Remedies

The general SLA remedies are available provided you meet your obligations as defined in this Services Description and all associated contract documents.

As described in the following tables, a credit will be issued as the sole remedy for failure to meet any of the SLAs described in the section above entitled "General SLA Availability", during any given calendar month. You may obtain no more than 100% of the monthly charge for the Services in a given calendar month.

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.

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

Web Security Availability per Calendar Month	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 Services at your discretion. Should the Services be terminated, such termination shall be the sole and exclusive remedy with respect to availability of the Services 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%, a credit will be issued in accordance with the following table:

Average Percentage of Web Content Scanning within 100 Milliseconds	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 Services at your discretion. Should the Services be terminated, such termination shall be the sole and exclusive remedy with respect to Web Latency.

3.5 Web Antivirus and Web Antispyware

If selected by you in the Schedule, IBM will provide Web Antivirus and Web Antispyware to assist you 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 Schedule.

3.5.1 IBM Web Antivirus and Web Antispyware Responsibilities

Activity 1 - Initialisation and Notification

IBM will provide access to Web Antivirus and Web Antispyware via the IP Addresses from which your Web traffic originates ("scanning IPs"). Your scanning IPs will be used to identify your Web traffic and to select your specific settings. IBM will not perform scans on files or content that does not originate from your 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 Web Security. Other content routed through HTTP (i.e., streaming media and/or HTTPS/SSL) may also be passed through 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 you request, a Web administrator, of a file download found to contain a Virus or Spyware in your Internet communications.

3.5.2 Your Web Antivirus and Web Antispyware Responsibilities

You agree to:

a. implement and maintain the configuration settings required to direct external traffic through Web Security; and

b. ensure your internal HTTP and FTP-over-HTTP traffic is not directed via Web Antivirus and Web Antispyware. If your Internet service mandates a direct connection rather than via a proxy, it is your responsibility to make the necessary changes to your infrastructure to facilitate such direct connection.

3.5.3 Service Level Agreements

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

The SLA remedies are available provided you meet your obligations as defined in this Services Description.

SLA

- Known Virus Protection – IBM will block all Known Viruses.

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

  If a Web transaction containing a Known Virus is detected but not stopped, IBM may promptly notify you and provide sufficient information to enable you to identify and delete the item. If infection is prevented, this SLA will be deemed met. If you fail 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 your systems are infected by one or more Viruses in a single calendar month during the contract period, a credit will be issued as specified in the Schedule. Such credit will only apply if you have provided notice to IBM, and IBM has confirmed and logged that a Virus has been passed to you through the Services. This remedy shall not apply to any deliberate self-infection by you.

3.6 Web URL Filtering

If selected by you in the Schedule, IBM will provide Web URL Filtering to assist you in denying User access to a Web page or attachment inline with your access restriction policy. Web URL Filtering is limited to the number of Users specified in the Schedule.

3.6.1 IBM Web URL Filtering Responsibilities

Activity 1 - Initialisation and Notification

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

3.6.2 Your Web URL Filtering Responsibilities

You agree to:

a. configure Web URL Filtering to include your access restriction policies, which should be based both on categories and types of content;

b. distribute and create your access restriction polices (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 your Internet service mandates a direct connection rather than via a proxy, it is your responsibility to make the necessary changes to your infrastructure to facilitate such direct connection.