

**IBM Application Security Services –  
Secure Web Gateway Management - Standard**

# Table of Contents

<b>1.</b>	<b>Scope of Services .....</b>	<b>4</b>
<b>2.</b>	<b>Definitions.....</b>	<b>4</b>
<b>3.</b>	<b>Services .....</b>	<b>4</b>
3.1	Security Operations Centers .....	5
3.2	Portal.....	5
3.2.1	IBM Portal Responsibilities.....	5
3.2.2	Your Portal Responsibilities .....	5
3.3	Services Contacts .....	5
3.3.1	IBM Services Contacts Responsibilities .....	6
3.3.2	Your Services Contacts Responsibilities .....	7
3.4	Security Intelligence .....	8
3.4.1	IBM Security Intelligence Responsibilities .....	8
3.4.2	Your Security Intelligence Responsibilities.....	8
3.5	Deployment and Activation.....	8
3.5.1	IBM Deployment and Activation Responsibilities .....	8
3.5.2	Your Deployment and Activation Responsibilities .....	11
3.6	Collection and Archival.....	12
3.6.1	IBM Collection and Archival Responsibilities.....	12
3.6.2	Your Collection and Archival Responsibilities .....	12
3.7	Policy Management.....	13
3.7.1	IBM Policy Management Responsibilities.....	13
3.7.2	Your Policy Management Responsibilities .....	14
3.8	Managed Agent Health and Availability Monitoring .....	14
3.8.1	IBM Managed Agent Health and Availability Monitoring Responsibilities.....	14
3.8.2	Your Managed Agent Health and Availability Monitoring Responsibilities.....	15
3.9	Agent Management.....	16
3.9.1	IBM Agent Management Responsibilities.....	16
3.9.2	Your Agent Management Responsibilities.....	16
3.10	Security Reporting.....	16
3.10.1	IBM Security Reporting Responsibilities.....	16
3.10.2	Your Security Reporting Responsibilities .....	17
<b>4.</b>	<b>Optional Services .....</b>	<b>17</b>
4.1	Out-of-Band Access .....	17
4.1.1	IBM Out-of-Band Access Responsibilities .....	17
4.1.2	Your Out-of-Band Access Responsibilities.....	17
4.2	Cold Standby.....	17
4.2.1	IBM Cold Standby Responsibilities.....	17
4.2.2	Your Cold Standby Responsibilities .....	18
4.3	Warm Standby .....	18
4.3.1	IBM Warm Standby Responsibilities .....	18
4.3.2	Your Warm Standby Responsibilities .....	18
4.4	High Availability.....	19
4.4.1	IBM High Availability Responsibilities.....	19
4.4.2	Your High Availability Responsibilities.....	19
4.5	Ticket System Integration.....	20
4.5.1	IBM Ticket System Integration Responsibilities.....	20

4.5.2	Your Ticket System Integration Responsibilities .....	20
4.6	Security Event and Log Delivery .....	20
4.6.1	IBM Security Event and Log Delivery Responsibilities .....	20
4.6.2	Your Security Event and Log Delivery Responsibilities .....	20
<b>5.</b>	<b>Service Level Agreements.....</b>	<b>20</b>
5.1	SLA Availability .....	20
5.2	SLA Remedies .....	21

## Services Description

### IBM Application Security Services - Secure Web Gateway Management - Standard

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/us/iss/html/contracts\\_worldwide\\_landing.html](http://www-935.ibm.com/services/us/iss/html/contracts_worldwide_landing.html) (on this page, please select your country in order to navigate to the country specific terms)

and incorporated herein by reference.

#### 1. Scope of Services

IBM Application Security Services - Secure Web Gateway Management - Standard (called “SWG - Standard” or “Services”) is designed to provide comprehensive Web content control and protection for your secure Web gateway devices (called “Agents”) across a variety of platforms and technologies. Such Agents must not be used for any other purpose while under management by IBM.

The Services features described herein are dependent upon the availability and supportability of products and product features being utilized. 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 (“IBM MSS”) portal (called “Portal”).

**antispam** – is designed to minimize the volume of spam e-mail to user mail boxes

**antivirus** – is designed to scan many kinds of file transfers (such as Web pages, e-mail traffic, and file transfer protocol (“FTP”) exchanges) for worms, viruses, and other forms of malware.

**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 or on behalf of IBM. Where applicable, Education Materials may include participant manuals, exercise documents, lab documents and presentation slides provided by IBM.

**Web filtering** – is designed to help the Services Recipient block objectionable content, mitigate Web-borne threats, and govern Web viewing behavior of personnel behind the managed Agent.

#### 3. Services

The following table highlights the measurable Services features. The subsequent sections provide narrative descriptions of each Services feature.

##### Services Feature Summary

Services Feature	Metric or Qty	Service Level Agreements
<a href="#">Services availability</a>	100%	<a href="#">Services availability SLA</a>
<a href="#">IBM MSS Portal availability</a>	99.9%	<a href="#">IBM MSS Portal availability SLA</a>
<a href="#">Authorized Security Contacts</a>	3 users	N/A
<a href="#">Log/event archival</a>	up to 7 years (1 year default)	N/A
<a href="#">Policy change request</a>	2 per month	N/A
<a href="#">Policy change request acknowledgement</a>	2 hours	<a href="#">Policy change request acknowledgement SLA</a>

<a href="#">Policy change request implementation</a>	24 hours	<a href="#">Policy change request implementation SLA</a>
<a href="#">Agent health alerting</a>	30 minutes	<a href="#">System monitoring SLA</a>
<a href="#">Content updates</a>	72 hours	<a href="#">Content update SLA</a>

### 3.1 Security Operations Centers

IBM Managed Security Services are delivered from a network of IBM Security Operations Centers (“SOCs”). IBM will provide access to the SOCs 24 hours/day, 7 days/week.

### 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 merchantability, 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) Agent configuration and policy details;
  - (3) security incident and service ticket information;
  - (4) ticketing and workflow initiation and updates;
  - (5) live chat and collaboration with SOC analysts;
  - (6) a template-driven reporting dashboard;
  - (7) access to real-time and archived Agent logs and events;
  - (8) authorization to download log data;
  - (9) granular security event and log query capabilities; and
  - (10) access to Education Materials in accordance with the terms provided in the Portal; and
- b. maintain availability of the Portal in accordance with the metrics provided in the section of this Services Description entitled “[Service Level Agreements](#)”, “[Portal Availability](#)”.

#### 3.2.2 Your Portal Responsibilities

You agree to:

- a. utilize 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 unauthorized 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 Services Contacts

You may choose from multiple levels of access to the SOC and the Portal to accommodate varying roles within your organization.

### **Authorized Security Contacts**

An Authorized Security Contact is defined as a decision-maker on all operational issues pertaining to IBM Managed Security Services.

### **Designated Services Contacts**

A Designated Services Contact is defined as a decision-maker on a subset of operational issues pertaining to IBM Managed Security Services, an Agent, or a group of Agents. IBM will only interface with a Designated Services Contact regarding operational activities that fall within the subset for which such contact is responsible (for example, designated Agent outage contact).

### **Portal Users**

IBM provides multiple levels of access for Portal users. These levels of access can be applied to an IBM Managed Security Service, an Agent, or a group of Agents. Portal users will be authenticated via static password or a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

## **3.3.1 IBM Services Contacts Responsibilities**

### **Authorized Security Contacts**

IBM will:

- a. allow you to create up to three Authorized Security Contacts;
- b. provide each Authorized Security Contact with:
  - (1) administrative Portal permissions to your Agents;
  - (2) the authorization to create unlimited Designated Services Contacts and Portal users;
  - (3) the authorization to delegate responsibility to Designated Services Contacts;
- c. interface with Authorized Security Contacts regarding support and notification issues pertaining to the Services; and
- d. verify the identity of Authorized Security Contacts using an authentication method that utilizes a pre-shared challenge pass phrase.

### **Designated Services Contacts**

IBM will:

- a. verify the identity of Designated Services Contacts using an authentication method that utilizes a pre-shared challenge pass phrase; and
- b. interface only with Designated Services Contacts regarding the subset of operational issues for which such contact is responsible.

### **Portal Users**

IBM will:

- a. provide multiple levels of access to the Portal:
  - (1) administrative user capabilities which will include:
    - (a) creating Portal users;
    - (b) creating and editing custom Agent groups;
    - (c) submitting policy change requests to the SOCs for a managed Agent or a group of Agents;
    - (d) submitting Services requests to the SOCs;
    - (e) "live chat" communicating with SOC analysts regarding specific incidents or tickets, generated as part of the Services;
    - (f) creating internal Services-related tickets and assigning such tickets to Portal users;
    - (g) querying, viewing, and updating Services-related tickets;
    - (h) viewing and editing Agent details;
    - (i) viewing Agent policies;

- (j) creating and editing vulnerability watch lists;
- (k) querying security event and log data;
- (l) scheduling downloads of security event and log data;
- (m) scheduling and running reports;
- (2) regular user capabilities which will include all of the capabilities of an administrative user, for the Agents to which they have been assigned, with the exception of creating Portal users ;
- (3) restricted user capabilities which will include all of the capabilities of a regular user, for the Agents to which they have been assigned, with the exception of:
  - (a) creating and submitting policy change requests;
  - (b) updating tickets; and
  - (c) editing Agent details;
- b. provide you with authorization to apply levels of access to an Agent or groups of Agents;
- c. authenticate Portal users using static password; and
- d. authenticate Portal users using a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

### **3.3.2 Your Services Contacts Responsibilities**

#### **Authorized Security Contacts**

You agree:

- a. to provide IBM with contact information for each Authorized Security Contact. Such Authorized Security Contacts will be responsible for:
  - (1) creating Designated Services Contacts and delegating responsibilities and permissions to such contacts, as appropriate;
  - (2) creating Portal users;
  - (3) authenticating with the SOCs using a pre-shared challenge pass phrase; and
  - (4) maintaining notification paths and your contact information, and providing such information to IBM;
- b. to ensure at least one Authorized Security Contact is available 24 hours/day, 7 days/week;
- c. to update IBM within three calendar days when your contact information changes; and
- d. and acknowledge that you are permitted to have no more than three Authorized Security Contacts regardless of the number of IBM services or Agent subscriptions for which you have contracted.

#### **Designated Services Contacts**

You agree:

- a. to provide IBM with contact information and role responsibility for each Designated Services Contact. Such Designated Services Contacts will be responsible for authenticating with the SOCs using a pass phrase; and
- b. and acknowledge that a Designated Services Contact may be required to be available 24 hours/day, 7 days/week based on the subset of responsibilities for which it is responsible (i.e., Agent outage).

#### **Portal Users**

You agree:

- a. that Portal users will use the Portal to perform daily operational Services activities;
- b. to be responsible for providing IBM-supported RSA SecureID tokens (as applicable); and
- c. and acknowledge the SOCs will only interface with Authorized Security Contacts and Designated Services Contacts.

### 3.4 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 customized 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 individualized alerts, advisories and security news.

#### 3.4.1 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.

#### 3.4.2 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; and
- c. access the Threat IQ.

### 3.5 Deployment and Activation

During deployment and activation, IBM will work with you to deploy a new Agent or begin management of an existing Agent.

Note: Deployment and Activation activities are performed one time during the performance of the services. If you choose to replace, upgrade, or move your Agent during the Services contract, IBM may require that such Agent be redeployed and reactivated (called "Redeployment"). Such Redeployments will be provided at an additional charge as specified in the Schedule. Redeployment charges apply only to hardware replacements, upgrades, or moves that you initiate. Such charges do not apply to Agent failures resulting in Agent Return Material Authorization ("RMA") activities.

#### 3.5.1 IBM Deployment and Activation Responsibilities

##### **Activity 1 - Project Kickoff**

The purpose of this activity is to conduct a project kickoff call. IBM will send you a welcome e-mail and conduct a kickoff call, for up to one hour for up to three of your personnel, to:

- a. introduce your Point of Contact to the assigned IBM deployment specialist;
- b. review each party's respective responsibilities;
- c. set schedule expectations; and

- d. begin to assess your requirements and environment.

**Completion Criteria:**

This activity will be complete when IBM has conducted the project kickoff call.

**Deliverable Materials:**

- None

**Activity 2 - Network Access Requirements**

The purpose of this activity is to establish network access requirements.

IBM will:

- a. provide you with a document called "Network Access Requirements", detailing:

- (1) how IBM will connect remotely to your network;
- (2) specific technical requirements to enable such remote connectivity;

Note: IBM may make changes to the "Network Access Requirements" document, as it deems appropriate, throughout the performance of the Services.

- b. connect to your network through the Internet, using IBM standard access methods; and
- c. if appropriate, utilize a site-to-site virtual private network ("VPN") to connect to your network. Such VPN may be provided by IBM for an additional charge as specified in the Schedule.

**Completion Criteria:**

This activity will be complete when IBM has provided your Point of Contact with the Network Access Requirements document.

**Deliverable Materials:**

- Network Access Requirements document

**Activity 3 - Assessment**

The purpose of this activity is to perform an assessment of your current environment, and business and technology goals, to help develop the required security strategy for the Agent.

**Task 1 - Gather Data**

IBM will:

- a. provide your Point of Contact with a data gathering form on which you will be asked to document:
  - (1) team member names, contact information, roles and responsibilities;
  - (2) unique country and site requirements;
  - (3) your existing network infrastructure;
  - (4) critical servers;
  - (5) number and type of end users; and
  - (6) key business drivers and/or dependencies that could influence Services delivery or timelines.

**Task 2 - Assess Environment**

IBM will:

- a. use the information provided in the data gathering form to assess your existing environment;
- b. determine an optimal Agent configuration; and
- c. if applicable, provide recommendations to adjust the policy of an Agent or layout of the network to enhance security.

**Task 3 - Assess Existing Agent**

IBM will:

- a. remotely assess the Agent to verify it meets IBM specifications;
- b. identify application and user accounts to be removed or added, as applicable;
- c. for Agents not meeting IBM's specifications:
  - (1) identify Agent software requiring upgrading, and/or

- (2) identify Agent hardware requiring upgrading to meet applicable vendor compatibility lists.

**Completion Criteria:**

This activity will be complete when IBM has assessed your environment and existing Agent (as applicable).

**Deliverable Materials:**

- None

**Activity 4 - Implementation**

The purpose of this activity is to implement the Agent.

**Task 1 - Configure the Agent**

IBM will:

- a. remotely assess the Agent to verify it meets IBM specifications;
- b. identify Agent software, hardware, and/or content that does not meet current IBM-supported levels;
- c. as appropriate, identify required hardware upgrades to support applicable vendor hardware compatibility lists;
- d. remotely configure the Agent, including setting the policy, hardening the operating system, and registering the Agent with the IBM MSS infrastructure;
- e. provide live phone support and location of vendor documents to assist you in configuring the Agent with a public IP address and associated settings. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;
- f. adjust the Agent policy to reduce the number of erroneous alarms (if applicable); and
- g. at your request, exercise the configuration and policy on the existing Agent.

**Task 2 - Install the Agent**

IBM will:

- a. provide live support, via phone and/or e-mail, to assist you in locating applicable vendor documents that detail physical installation procedures and cabling. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;
- b. provide recommendations to adjust the layout of the network to enhance security (as applicable);
- c. remotely configure the Agent, including registering the Agent with the IBM MSS infrastructure; and
- d. adjust the Agent policy to reduce the number of erroneous alarms (if applicable).

Note: You may contract separately for IBM to provide physical installation services.

**Completion Criteria:**

This activity will be complete when the Agent is registered with the IBM MSS infrastructure.

**Deliverable Materials:**

- None

**Activity 5 - Testing and Verification**

The purpose of this activity is to perform testing and verification of the Services.

IBM will:

- a. verify connectivity of the Agent to the IBM MSS infrastructure;
- b. perform Services acceptance testing;
- c. verify delivery of log data from the Agent to the IBM MSS infrastructure;
- d. verify availability and functionality of the Agent in the Portal;
- e. perform quality assurance testing of the Agent; and
- f. remotely demonstrate the primary features of the Portal for up to ten of your personnel, for up to one hour.

**Completion Criteria:**

This activity will be complete when IBM has verified availability and functionality of the Agent in the Portal.

***Deliverable Materials:***

- None

**Activity 6 - Services Activation**

The purpose of this activity is to activate the Services.

IBM will:

- assume management and support of the Agent;
- set the Agent to “active”; and
- transition the Agent to the SOCs for ongoing management and support.

***Completion Criteria:***

This activity will be complete when the Agent is set to “active”.

***Deliverable Materials:***

- None

**3.5.2 Your Deployment and Activation Responsibilities**

**Activity 1 - Project Kickoff**

You agree to:

- attend the project kickoff call; and
- review each party’s respective responsibilities.

**Activity 2 - Network Access Requirements**

You agree to:

- review and comply with the IBM “Network Access Requirements” document during deployment and throughout the term of the contract; and
- be solely responsible for any charges incurred as a result of IBM utilizing a site-to-site VPN to connect to your network.

**Activity 3 - Assessment**

***Task 1 - Gather Data***

You agree to:

- complete and return any questionnaires and/or data gathering forms to IBM within five days of your receipt;
- obtain and provide applicable information, data, consents, decisions and approvals as required by IBM to perform the Services deployment, within two business days of IBM’s request;
- work in good faith with IBM to accurately assess your network environment;
- provide contacts within your organization, and specify a notification path through your organization, in the event IBM must contact you; and
- update IBM within three calendar days when your contact information changes.

***Task 2 - Assess Environment***

You agree:

- to maintain current licensing, and support and maintenance for the Agents; and
- to perform all IBM-requested changes to your network layout to enhance security.

***Task 3 - Assess Existing Agent***

You agree:

- to ensure the existing Agent meets IBM’s specifications;
- to remove or add IBM-specified applications and user accounts;
- if requested by IBM:
  - (1) to upgrade IBM-specified Agent software; and

- (2) to upgrade IBM-specified Agent hardware.

#### **Activity 4 - Implementation**

##### ***Task 1 - Configure the Agent***

You agree to:

- a. update Agent software or content to the most current IBM-supported version (i.e., physically load media as applicable);
- b. update hardware to support applicable vendor hardware compatibility lists (if applicable);
- c. adjust the Agent policy as requested by IBM;
- d. configure the Agent with a public IP address and associated settings; and
- e. assist IBM in exercising the existing Agent configuration and policy (if applicable).

##### ***Task 2 - Install the Agent***

You agree:

- a. to work with IBM in locating vendor documents that detail physical installation procedures and cabling. You will schedule such support in advance to ensure availability of an IBM deployment specialist;
- b. to be responsible for the physical cabling and installation of the Agent(s); and
- c. to perform any IBM-specified adjustments to the layout of the network to enhance security.

#### **Activity 5 - Testing and Verification**

You agree:

- a. to be responsible for development of all of your specific acceptance testing plans;
- b. to be responsible for performing acceptance testing of your applications and network connectivity; and
- c. and acknowledge that additional acceptance testing performed by you, or lack thereof, does not preclude IBM from setting the Agent to "active" in the SOCs for ongoing support and management.

#### **Activity 6 - Services Activation**

No additional responsibilities are required by you for this activity.

### **3.6 Collection and Archival**

IBM utilizes the X-Force Protection System for collecting, organizing, archiving and retrieving security event and log data. The Portal provides you with a 24 hours/day, 7 days/week view into the Services, including online access to raw logs collected and stored within the X-Force Protection System infrastructure. Security event and log data will be viewable online in the Portal for one year. At the end of the one year period, the data will be transitioned to offline storage (if applicable).

#### **3.6.1 IBM Collection and Archival Responsibilities**

IBM will:

- a. collect log and event data generated by the managed Agent as such data reaches the IBM MSS infrastructure;
- b. throttle log and event data streams generated by the managed Agent when such data streams exceed 100 events per second ("EPS");
- c. uniquely identify collected log and event data;
- d. archive collected data in the X-Force Protection System;
- e. provide one year of log and event data storage unless otherwise specified by you;
- f. display collected log and event data in the Portal for one year;
- g. where supported, normalize the log and event data for enhanced presentation in the Portal;
- h. begin purging collected log and event data using a first in, first out ("FIFO") method:
  - (1) based on the default (one year) retention period or your defined retention periods (if applicable); or
  - (2) when the log and event data age has exceeded seven years;

Note: Notwithstanding any retention periods defined by you, IBM will not retain log and event data for more than seven years. If you exceed your seven year retention period at any time during the contract period, IBM will begin purging the collected log and event data using the FIFO method.

- i. if it deems it appropriate, recommend a site-to-site VPN be utilized to encrypt traffic that is not natively encrypted by the Agent.

Note: Data traveling across the Internet is encrypted using industry-standard encryption algorithms provided natively by the Agent only when the Agent (provided by you) is equipped with the capability to do so.

### 3.6.2 Your Collection and Archival Responsibilities

You agree:

- a. to provide IBM with security event and log retention periods not to exceed seven years;
- b. to use the Portal to review and query security event and log data;
- c. to use the Portal to maintain available log and event storage space awareness;
- d. to ensure an active SWG - Standard contract is being maintained for each unique security event and log source; and

Note: If the Services are terminated for any reason whatsoever, IBM will be relieved of its obligation to store your security event and log data.

- e. and acknowledge that:
  - (1) unless otherwise specified in writing by you, IBM will maintain the collected log and event data for one calendar year;
  - (2) all log and event data will be transmitted to the SOCs via the Internet;
  - (3) should you choose not to utilize an IBM-recommended site-to-site VPN for Agents that do not provide encryption algorithms natively, unencrypted data traveling across the Internet will not be encrypted;
  - (4) IBM can only collect and archive log and event data that successfully reaches the IBM MSS infrastructure;
  - (5) IBM does not guarantee the legal submission of any security event or log data into any domestic or international legal system. Admissibility of evidence is based on the technologies involved and your ability to prove proper data handling and chain of custody for each set of data presented;
  - (6) IBM has the right to throttle event streams generated by the Agent that exceed 100 EPS (if required);
  - (7) IBM will not store log and event data for more than seven years; and
  - (8) your defined retention periods may not exceed seven years. IBM will begin purging data using the FIFO method when collected log and event data exceeds seven years, regardless of your specified retention periods.

## 3.7 Policy Management

IBM defines a single rule-based Agent policy/configuration change as any authorized request for the addition or modification of one rule on one context with five or fewer objects in a single request. A change request requiring the addition of six or more objects or the manipulation of two or more rules will be counted as two or more requests. If the request applies to changes outside of the rule-based Agent policy, each submitted request will be considered a single change.

You may configure the managed Agent with a single global policy that applies to all ports.

### 3.7.1 IBM Policy Management Responsibilities

IBM will:

- a. accept up to two policy change requests per month from Authorized Security Contacts or Designated Services Contacts, via the Portal;
- b. acknowledge policy change requests via the Portal within the timeframes established in the section of this Services Description entitled "[Service Level Agreements](#)", "[Policy change request acknowledgement](#)";

- c. review submitted policy change requests to verify you have provided all required information in such requests;
- d. if necessary, notify the submitter that additional information is needed. During this time, service level agreement (“SLA”) timers will be placed on hold;
- e. prepare and review the policy change configuration as requested by you;
- f. implement policy change requests within the timeframes established in the section of this Services Description entitled “[Service Level Agreements](#)”, “[Policy change request implementation](#)”;
- g. document details of the policy change request in the IBM MSS ticketing system;
- h. display policy change request tickets in the Portal;
- i. at your request, and for an additional charge (and subject to availability of IBM resource), provide additional policy changes;
- j. perform daily configuration backup of the managed Agent;
- k. maintain 14 configuration backups;
- l. display the current configuration of the Agent in the Portal; and
- m. on a quarterly basis upon your written request:
  - (1) audit your policy settings to verify accuracy; and
  - (2) work with you to review Agents under management and provide recommended changes to the network protection strategy.

### **3.7.2 Your Policy Management Responsibilities**

You agree:

- a. to ensure all policy change requests are submitted by an Authorized Security Contact or a Designated Services Contact, using the Portal, in accordance with the established procedures identified above;
- b. to be responsible for providing sufficient information for each requested policy change to allow IBM to successfully perform such change;
- c. to be responsible for notifying IBM if you wish IBM to perform a quarterly policy review;
- d. to be solely responsible for your own security strategy, including security incident response procedures; and
- e. and acknowledge:
  - (1) all policy changes will be completed by IBM and not by you;
  - (2) implementation of policy changes that IBM has deemed as having an adverse impact on the Agents’ ability to protect the network environment will result in the suspension of applicable SLAs; and
  - (3) following closure of a calendar month, unused changes are considered void and may not be rolled over to the following month.

## **3.8 Managed Agent Health and Availability Monitoring**

IBM will monitor the health status and availability of the managed Agents. Such monitoring is designed to assist in increasing availability and uptime of the Agents.

### **3.8.1 IBM Managed Agent Health and Availability Monitoring Responsibilities**

#### **Activity 1 - Monitoring**

The purpose of this activity is to monitor the health and performance of the Agents. IBM MSS will perform this task using either Agent-based monitoring or Agentless monitoring.

#### **Agent-Based Monitoring**

When technically feasible, IBM will install software on eligible Agents to monitor system health and performance, and report metrics back to the SOCs.

IBM will:

- a. for eligible platforms, install monitoring software on the Agents;

- b. analyze and respond to key metrics, which may include:
  - (1) hard disk capacity;
  - (2) CPU utilization;
  - (3) memory utilization; and
  - (4) process availability; and
- c. respond to alerts generated by the monitoring software.

#### **Agentless Monitoring**

When it is not technically feasible to install monitoring software, IBM will monitor the data stream coming from the Agents and/or poll administrative interfaces on the Agents.

IBM will:

- a. monitor the administrative interfaces of the Agents; and/or
- b. monitor the event stream generated by the Agents; and
- c. initiate additional time-based checks if contact with a managed Agent is lost.

#### **Activity 2 - Troubleshooting**

The purpose of this activity is to perform research and investigation if the Agents do not perform as expected or a potential Agent health issue is identified.

IBM will:

- a. create a trouble ticket in the event of an Agent performance problem or potential Agent health issue;
- b. begin research and investigation of the documented issue;
- c. if the Agent is identified as the potential source of a network-related problem, examine the Agent configuration and functionality for potential issues; and
- d. display the Agent health and outage ticket in the Portal.

#### **Activity 3 - Notification**

The purpose of this activity is to notify you if the Agent becomes unreachable through standard in-band means.

IBM will:

- a. notify you if the Agent becomes unreachable through standard in-band means. Such notification will be via telephone using a predetermined notification procedure within the timeframe established in the section of this Services Description entitled "[Service Level Agreements](#)", "[Proactive system monitoring](#)";
- b. begin investigation of problems related to the configuration or functionality of the Agent, following initiation of telephone notification; and
- c. display Agent health and outage tickets in the Portal.

### **3.8.2 Your Managed Agent Health and Availability Monitoring Responsibilities**

#### **Activity 1 - Monitoring**

You agree to:

- a. allow IBM to install monitoring software on all managed Agents, where such installation is deemed by IBM to be technically feasible; or
- b. allow IBM to monitor the administrative interfaces and event stream of the managed Agents when it is not technically feasible to install monitoring software on such Agents.

#### **Activity 2 - Troubleshooting**

You agree:

- a. to participate in troubleshooting sessions with IBM (as required);
- b. to be responsible for providing all remote configuration and troubleshooting, if you have elected not to implement an Out-of-Band ("OOB") solution, or if the OOB solution is unavailable for any reason; and

- c. and acknowledge that if the managed Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

### **Activity 3 - Notification**

You agree to:

- a. provide your notification paths and contact information;
- b. update IBM within three calendar days when your contact information changes; and
- c. ensure an Authorized Security Contact or Agent outage Designated Services Contact is available 24 hours/day, 7 days/week.

## **3.9 Agent Management**

Agent application and security updates are critical components of an enterprise. IBM uses a vendor agnostic approach to Agent management.

### **3.9.1 IBM Agent Management Responsibilities**

IBM will:

- a. be the sole provider of software-level management for the Agents;
- b. maintain system status awareness;
- c. install new security content updates on the Agents, as they become generally available from the applicable vendor, within the timeframe established in the section of this Services Description entitled "Service Level Agreements", "Proactive security content update";
- d. install patches and software updates in order to improve performance, enable additional functionality, or resolve an application problem. IBM assumes no responsibility for, and makes no warranties concerning, vendor-provided patches, updates or security content;
- e. declare a maintenance window in advance of Agent updates that may require platform downtime or your assistance to complete; and
- f. clearly state, within the maintenance window notification, the expected impacts of a scheduled maintenance and your specific requirements.

### **3.9.2 Your Agent Management Responsibilities**

You agree:

- a. to perform IBM-specified hardware upgrades to support the current software and firmware;
- b. to work with IBM to perform Agent updates (as required);
- c. to be responsible for all charges associated with hardware upgrades;
- d. to maintain current licensing, and support and maintenance contracts;
- e. to ensure appropriate consents are in place with your vendors to allow IBM to leverage existing support and maintenance contracts on your behalf. If such agreements are not in place, IBM will not be able to contact the vendor directly to resolve support issues; and
- f. and acknowledge:
  - (1) all updates are transmitted and applied via the Internet;
  - (2) if vendor consents are not obtained or are revoked at any point during the contract period, Services and/or SLAs may be suspended by IBM;
  - (3) noncompliance with IBM-required software upgrades may result in suspension of Services delivery and/or SLAs; and
  - (4) noncompliance with IBM-required hardware upgrades may result in suspension of Services delivery and/or SLAs.

## **3.10 Security Reporting**

Utilizing the Portal, you will have access to Services information and reporting with customizable views of activity at the enterprise, work group and Agent levels. The Portal also provides you with the ability to schedule customized reporting.

### **3.10.1 IBM Security Reporting Responsibilities**

IBM will provide you with access to reporting capabilities in the Portal which include:

- a. number of SLAs invoked and met;
- b. number, types, and summary of Services requests/tickets; and
- c. system logs.

### **3.10.2 Your Security Reporting Responsibilities**

You agree to:

- a. generate Services-related reports using the Portal; and
- b. be responsible for scheduling reports (as applicable).

## **4. Optional Services**

Optional services selected by you, and any additional charges for such services, will be specified in the Schedule.

### **4.1 Out-of-Band Access**

OOB access is a highly recommended feature that assists the SOCs if connectivity to an Agent is lost. If such connectivity problems occur, the SOC analysts can dial into the modem to verify the Agent is functioning properly and assist in determining the source of the outage before escalating to you.

#### **4.1.1 IBM Out-of-Band Access Responsibilities**

At your request, for no additional charge, IBM will:

- a. provide live support, via phone and e-mail, to assist you in locating applicable vendor documents which detail physical installation procedures and cabling;
- b. configure the OOB device to access the managed Agents; or
- c. work in good faith with you to utilize an IBM-approved existing OOB solution.

#### **4.1.2 Your Out-of-Band Access Responsibilities**

You agree:

- a. for new OOB solutions:
  - (1) to purchase an IBM-supported OOB device;
  - (2) to physically install and connect the OOB device to the Agent;
  - (3) to provide a dedicated analog telephone line for access;
  - (4) to physically connect the OOB device to the dedicated telephone line and maintain the connection;
  - (5) to be responsible for all charges associated with the OOB device and telephone line; and
  - (6) to be responsible for all charges associated with the ongoing management of the OOB solution;
- b. for existing OOB solutions:
  - (1) to ensure the solution does not allow IBM to access non-managed devices;
  - (2) to ensure the solution does not require installation of specialized software;
  - (3) to provide IBM with detailed instructions for accessing managed Agents; and
  - (4) to be responsible for all aspects of managing the OOB solution;
- c. and acknowledge that existing OOB solutions must be approved by IBM;
- d. to maintain current support and maintenance contracts for the OOB (as required); and
- e. to be responsible for providing all remote configuration and troubleshooting, if you elect not to implement an OOB solution or if the OOB solution is unavailable for any reason.

### **4.2 Cold Standby**

Cold standby is a method of disaster recovery whereby a spare Agent is available as a substitute in the event the primary Agent has a hardware and/or software failure. Cold standby Agents are not powered or ready for use, and do not contain active configuration, policy, or content updates.

#### **4.2.1 IBM Cold Standby Responsibilities**

At your request, for no additional charge, IBM will:

- a. work with you to transition the cold standby Agent to production and set such Agent to “active” in the event the primary Agent fails;
- b. apply required content updates to the cold standby Agent in the event the primary Agent fails; and
- c. apply the active current configuration to the Agent in the event the primary Agent fails.

#### **4.2.2 Your Cold Standby Responsibilities**

You agree:

- a. to provide a secondary Agent to act as a cold standby Agent;
- b. to maintain current licensing, and support and maintenance contracts, for the cold standby Agent;
- c. to work with IBM to transition the cold standby Agent to production and set such Agent to “active” in the event the primary Agent fails; and
- d. and acknowledge that:
  - (1) cold standby Agents are not managed and maintained by IBM unless they are transitioned to “active”;
  - (2) cold standby Agents require configuration changes in order to transition to “active”; and
  - (3) cold standby Agents may not generate traffic for the SOCs unless the primary Agent has failed and the cold standby Agent has been placed into production and transitioned to “active”.

### **4.3 Warm Standby**

Warm standby is a method of redundancy that can reduce downtime due to Agent hardware and/or software failures. Warm standby management is designed to provide you with the option of having IBM manage and keep up to date a single spare Agent. In the event your primary Agent fails, the spare or “warm” Agent will be on-hand to restore Services more quickly. A standby Agent may not generate any traffic for the SOCs unless it is placed into production and set to “active”.

IBM strongly encourages OOB access to the warm standby Agent as described in the section of this Services Description entitled “Out-of-Band Access”.

#### **4.3.1 IBM Warm Standby Responsibilities**

At your request, and for an additional charge specified in the Schedule, IBM will:

- a. maintain health and availability status of the warm standby Agent as described in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”;
- b. apply content updates to the warm standby Agents as described in the section of this Services Description entitled “Agent Management”; and
- c. transition the warm standby Agent to “active” in the event the primary Agent fails.

#### **4.3.2 Your Warm Standby Responsibilities**

You agree:

- a. to maintain current licensing, and support and maintenance contracts, for all warm standby platforms;
- b. to be responsible for all charges associated with ongoing management of the warm standby Agent;
- c. to provide secondary IP addressing;
- d. to comply with and perform Your Managed Agent Health and Availability Monitoring Responsibilities as described in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”;
- e. to comply with and perform Your Agent Management Responsibilities as defined in the section of this Services Description entitled “Agent Management”;
- f. and acknowledge that:
  - (1) policy changes made to the primary Agent will not be reflected on the warm standby Agent;
  - (2) standby Agents may not generate traffic for the SOCs unless they have been placed into production and set to “active”; and
- g. to be responsible for providing all remote configuration and troubleshooting, if you elect not to implement an OOB solution or if the OOB solution is unavailable for any reason.

#### 4.4 High Availability

To help protect against hardware and/or software failure and provide high availability (“HA”), two managed protection Agents may be configured and deployed; one fully operational and the other waiting as a backup to take over should the first Agent fail. Some Agents can also be deployed as clusters, such that multiple Agents operate and share network load.

##### **Active/Passive Implementations**

In this configuration, a second Agent is configured, ready to begin serving the network if the primary Agent experiences a critical hardware or software failure. In such a scenario, failover is automatic and expected to be immediate.

##### **Active/Active Implementations**

Active/active clusters use two or more Agents to handle the network traffic simultaneously. In this configuration, each Agent handles a share of the network packets, determined by a load-balancing algorithm. If one Agent fails, the other Agent(s) is/are designed to automatically handle all of the traffic until the failed Agent has been restored.

IBM strongly encourages OOB access to all Agents in the high availability configuration, as described in the section of this Services Description entitled “Out-of-Band Access”.

#### 4.4.1 IBM High Availability Responsibilities

At your request, and for an additional charge specified in the Schedule, IBM will:

- a. configure a secondary Agent in either an active/passive or active/active configuration, as specified by you;
- b. manage and monitor the HA solution;
- c. maintain health and availability status of the secondary Agent as described in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”;
- d. apply content updates to the secondary Agent(s) as described in the section of this Services Description entitled “Agent Management”; and
- e. update the policy of the secondary Agent as described in the section of this Services Description entitled “Policy Management”.

#### 4.4.2 Your High Availability Responsibilities

You agree:

- a. to provide a secondary Agent;
- b. to make any required changes to software licensing;
- c. to provide secondary IP addressing;
- d. to be responsible for all charges associated with ongoing management for the secondary Agent;
- e. to comply with and perform:
  - (1) Your Managed Agent Health and Availability Monitoring Responsibilities as defined in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”;
  - (2) Your Agent Management Responsibilities as defined in the section of this Services Description entitled “Agent Management”;
  - (3) Your Policy Management Responsibilities as defined in the section of this Services Description entitled “Policy Management”;
- f. to be responsible for providing all remote configuration and troubleshooting, you elect not to implement an OOB solution on both the primary and secondary Agents or if the OOB solution is unavailable for any reason; and
- g. and acknowledge that:
  - (1) the Services do not support non-integrated HA solutions;
  - (2) IBM supports active/active configurations utilizing three or more Agents in unicast mode only.

## **4.5 Ticket System Integration**

If you wish to leverage existing trouble ticketing and case management investments, IBM will provide an application program interface (“API”) which allows for customized integration with external ticketing systems.

### **4.5.1 IBM Ticket System Integration Responsibilities**

At your request, and for an additional charge specified in the Schedule, IBM will provide an API to allow for customized integration with external ticketing systems.

### **4.5.2 Your Ticket System Integration Responsibilities**

You agree:

- a. to be responsible for all additional charges associated with API ticket integration;
- b. to utilize the Portal API package to facilitate ticket integration;
- c. to be responsible for all engineering and development issues associated with ticket integration; and
- d. and acknowledge that IBM will not provide assistance or consulting for your ticketing system integration.

## **4.6 Security Event and Log Delivery**

At your request, IBM will retrieve log and event data from the IBM MSS infrastructure and make it available for download from a secured IBM server. In cases where the amount of log and event data is deemed by IBM to be too excessive to make available via download, IBM will store the data on encrypted media and ship it to a location you specify. The feasibility of delivery via download will be assessed on a case-by-case basis.

### **4.6.1 IBM Security Event and Log Delivery Responsibilities**

At your request, and for an additional charge specified in the Schedule, IBM will:

- a. upon your request (via the Portal), retrieve specified data from the IBM MSS infrastructure and make it available to you for download on a secured IBM server; and
- b. advise you of additional charges for all time and materials utilized to retrieve and prepare the data.

### **4.6.2 Your Security Event and Log Delivery Responsibilities**

You agree:

- a. to request security event log delivery via the Portal;
- b. to download requested data from a secured IBM server;
- c. and acknowledge that requests for retrieval of excessively large amounts of data may require data be stored on encrypted media and shipped to a location you specify; and
- d. to be responsible for all time and material charges, and shipping charges (as applicable) associated with log delivery.

## **5. Service Level Agreements**

IBM 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, the Agent has been set to “active”, and support and management of the Agent have been successfully transitioned to “active” in the SOCs. The SLA remedies are available provided you meet your obligations as defined in this Services Description and all associated contract documents.

### **5.1 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 “SLA Remedies”.

- a. Policy change request acknowledgement – IBM will acknowledge receipt of your policy change request within two hours of receipt by IBM. This SLA is only available for policy change requests submitted by an Authorized Security Contact or a Designated Services Contact in accordance with the established procedures documented in the Portal.

- b. Policy change request implementation – IBM will implement your policy change requests within 24 hours of receipt by IBM unless the request has been placed in a “hold” status due to insufficient information required to implement the submitted policy change request. This SLA is only available for policy change requests submitted by an Authorized Security Contact or a Designated Services Contact in accordance with the established procedures documented in the Portal.
- c. Proactive system monitoring – IBM will notify you within 30 minutes after IBM determines your Agent is unreachable via standard in-band connectivity.
- d. Proactive security content update – IBM will begin application of new security content updates within 72 hours after such update is published as generally available by the applicable vendor.
- e. Services availability – IBM will provide 100% service availability for the SOCs.
- f. Portal availability – IBM will provide 99.9% accessibility for the Portal outside of the times specified in the section of this Services Description entitled “Scheduled and Emergency Portal Maintenance”.

**5.2 SLA Remedies**

- a. Policy change request acknowledgement, policy change request implementation, proactive system monitoring, proactive security content update, services availability and Portal availability credits – If IBM fails to meet any of these SLAs, a credit will be issued for the applicable charges for one day of the monthly monitoring charge for the affected Agent for which the respective SLA was not met.

**SLAs and Remedies Summary**

Service Level Agreements	Availability Remedies
Policy change request acknowledgement	Credit of 1 day of the monthly monitoring charge for the affected Agent
Policy change request implementation	
Proactive system monitoring	
Proactive security content update	
Services availability	
Portal availability	